10-INTEL-07
July 21, 2010

Inspector General
United States Department of Defense

DEPUTY INSPECTOR GENERAL FOR INTELLIGENCE

DoD Efforts to Protect Critical Program Information
The Army's Warfighter Information Network - Tactical

~~FOR OFFICIAL USE ONLY~~

Additional Information and Copies

For information and to request copies of this report, contact the DoD Office of Inspector General at (703) 604-8841 or (DSN 664-8841).

Suggestions for Assessments

To suggest ideas for, or to request future audits or evaluations, contact the Office of the Deputy Inspector General for Intelligence at (703) 604-8800 (DSN 664-8800) or UNCLASSIFIED fax (703) 604-0045. Ideas and requests can also be mailed to:

ODIG-INTEL (ATTN: Intelligence Suggestions)
Department of Defense Inspector General
400 Army Navy Drive (Room 703)
Arlington, VA 22202-4704

To report fraud, waste, mismanagement, and abuse of authority.

Send written complaints to: Defense Hotline, The Pentagon, Washington, DC 20301-1900
Phone: 800.424.9098 e-mail: hotline@dodig.mil www.dodig.mil/hotline

Acronyms and Abbreviations

ARTPC	Army Research and Technology Protection Center
ASA(ALT)	Assistant Secretary of the Army (Acquisition, Logistics, and Technology
CPI	Critical Program Information
PM	Program Manager
RDA	Research, Development, and Acquisition
RDT&E	Research, Development, Test, and Evaluation
RTP	Research and Technology Protection
USD(AT&L)	Under Secretary of Defense (Acquisition, Technology, and Logistics)
WIN-T	Warfighter Information Network - Tactical

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

July 21, 2010

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: DoD Efforts to Protect Critical Program Information:
The Army's Warfighter Information Network – Tactical
(Report No. 10-INTEL-07)

We are providing this report for information and use. We considered management comments on a draft of this report in preparing the final report.

DoD Directive 7650.3 and Office of Management and Budget Circular No. A-50 require that recommendations be resolved promptly. While management generally concurred with our recommendations, many of the comments were only partially responsive because they lacked either a description of actions for accomplishing the recommendations or a date, and in some instances both. Therefore, we are requesting additional comments as indicated in the recommendations table on page ii by August 20, 2010.

If possible, please send a .pdf file containing your comments to DoD OIG - (b)(6) @dodig.mil. Copies of the management comments must contain the actual signature of the authorizing official. We are unable to accept the /Signed/ symbol in place of the actual signature. If you arrange to send classified comments electronically, you must send them over the SECRET Internet Protocol Router Network to DoD OIG - (b)(6) @dodig.smil.mil.

As a result of management comments, we redirected recommendations B2-2 and B6 to reflect the Deputy Under Secretary of Defense for HUMINT, Counterintelligence, and Security as the cognizant authority for management comments and recommendation B-8 to reflect the Under Secretary of Defense for Acquisition, Technology, and Logistics as the lead cognizant authority for management comments. We received management comments from the two agencies respectively.

We appreciate the courtesies extended to the staff. Please direct questions to DoD OIG - [redacted] at (703) 604- DoD OIG - (b)(6) (DSN 664- DoD OIG - (b)(6)) or [redacted] DoD OIG - (b)(6) at (703) 604- DoD OIG - (b)(6) (DSN 664- DoD OIG - (b)(6)).

(b)(6) [redacted]

Patricia A. Brannin
Deputy Inspector General
for Intelligence

DISTRIBUTION:

OFFICE OF THE SECRETARY OF DEFENSE
- Under Secretary of Defense (Acquisition, Technology, and Logistics)
- Under Secretary of Defense (Policy)
- Under Secretary of Defense (Intelligence)
- Assistant Secretary of Defense (Networks and Information Integration)/ DoD Chief Information Officer
- Deputy Under Secretary of Defense (HUMINT, Counterintelligence and Security)
- Director, Defense Security Service

DEPARTMENT OF THE ARMY
- Assistant Secretary of the Army (Acquisition, Logistics, and Technology)
- Commanding General, Army Materiel Command
  - G-2, Army Materiel Command
- Deputy Chief of Staff, G-2
- Inspector General, Department of the Army
- Auditor General, Department of the Army
- Program Executive Officer for Command, Control, and Communications Tactical
- Program Manager, Warfighter Information Network – Tactical

NON-DEFENSE ORGANIZATIONS
- Office of Management and Budget

CONGRESSIONAL COMMITTEES AND SUBCOMMITTEES, CHAIRMAN AND RANKING
- Senate Subcommittee on Defense, Committee on Appropriations
- Senate Committee on Armed Services
- Senate Select Committee on Intelligence
- Senate Committee on Homeland Security and Governmental Affairs
- House Committee on Armed Services
- House Permanent Select Committee on Intelligence
- House Committee on Oversight and Government Reform
- House Subcommittee on Government Management, Organization, and Procurement, Committee on Oversight and Government Reform
- House Subcommittee on National Security and Foreign Affairs, Committee on Oversight and Government Reform

Results in Brief: DoD Efforts to Protect Critical Program Information: The Army's Warfighter Information Network – Tactical

What We Did

This is the first in a series of assessments to determine how DoD protects critical program information (CPI). The Army's Warfighter Information Network – Tactical (WIN-T) is the first of three acquisition category ID programs of record to be used as a case study to assess the Department's effectiveness in protecting CPI. We conducted this assessment in coordination with DoD research, development, acquisition, counterintelligence (CI), and security subject matter experts. We analyzed key issue areas related to program protection, specifically: the ability to identify and protect CPI; manage the foreign visit program; apply program protection horizontally; train its workforce in program protection; and optimize intelligence, CI, and security resources, threat data, and policies to guide program protection efforts. Because the WIN-T program has no foreign involvement, that issue area was not relevant. We also assessed DoD program protection efforts for standardization of protection processes and their application, oversight of protection processes and responsibility for protection efforts.

What We Found

We found that while DoD and Army policy to protect CPI has progressed in recent years, there is still a need for improvement. The Army has a good process in place for identifying CPI through integrated product teams and the Army Research and Technology Protection Center. However, Army efforts to protect CPI are not integrated and synchronized to the greatest extent possible, and they are not optimizing the ability to provide uniform research and technology protection across the Army.

In addition, program officials were aware of horizontal protection but had some reservations about the security of the data; and the workforce had received training in program protection, but training needs to be more tailored. Also, program personnel used intelligence, CI, and security resources, threat data, and policies to guide program protection efforts; however, more coordination is needed among program, intelligence, CI, and security personnel – especially with Defense Security Service personnel - in order to optimize their efforts.

What We Recommend

The Under Secretaries of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) and for Intelligence (USD(I)), the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD (NII)/DoD CIO), and the Deputy Under Secretary of Defense for HUMINT, Counterintelligence, and Security (DUSD(HCI&S)) should develop policies related to CPI protection in the areas of anti-tamper; commercial off-the-shelf components; model contract language; standardized guidance for training, security requirements for contractors processing CPI on contractor information systems, and the host for the horizontal protection database. The Assistant Secretary of the Army for Acquisition, Logistics, and Technology (ASA(ALT)), the Commanding General, Army Materiel Command (CG, AMC), and the Deputy Chief of Staff (DCS), G-2 (Intelligence) should determine the most effective means to optimize Army research and technology protection efforts. The USD(I), should provide guidance on model language and use of the DD Form 254 to ensure access to and oversight of controlled unclassified CPI in defense industry.

Management Comments and Our Response

While comments from USD(AT&L), USD(I), ASD/NII, DUSD (HCI&S), ASA(ALT), Army Deputy Chief of Staff, G-2 (Intelligence) and CG, AMC generally concurred with our recommendations, many of the comments were only partially responsive because they lacked either a description of actions for accomplishing the recommendations, a date, and in some instances both in meeting the intent of the recommendations. Please see the recommendations table on the back of this page.

Recommendations Table

Management	Recommendations Requiring Comment	No Additional Comments Required
Under Secretary of Defense (Acquisition, Technology, and Logistics)	**B1-1, B1-2, B2-1, B-3, B5-1**	**B1-1, B1-2, B2-1, B3, B5-1, B8**
Under Secretary of Defense (Intelligence)	**B1-1**	**B1-1, B3, B5-1, B8**
Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer		**B1-1, B3, B5-1, B8**
Deputy Under Secretary of Defense (HUMINT, Counterintelligence, and Security)	**B2-2, B6**	**B2-2, B6**
Assistant Secretary of the Army (Acquisition, Logistics, and Technology)		**A**
Commanding General, Army Materiel Command		**A**
Army Deputy Chief of Staff, G-2 (Intelligence)		**A**

Please provide comments by August 13, 2010.

Table of Contents

Introduction

Protecting critical program information (CPI) is imperative in order for the U.S. to maintain the technologically-dependent cutting edge of its weapon systems. Critical program information is defined as elements or components of a research, development, or acquisition (RDA) program that, if compromised, could cause significant degradation in mission effectiveness; shorten the expected combat-effective life of the system; reduce technological advantage; significantly alter program direction; or enable an adversary to defeat, counter, copy, or reverse-engineer the technology or capability. Critical program information includes information about applications, capabilities, processes, and end items; elements or components critical to a military system's or network's mission effectiveness; and technology that would reduce the U.S. technological advantage if it came under foreign control.

Objective

The objective of this program protection assessment pilot was to determine how effectively DoD identifies and protects CPI. Specifically, we assessed the following eight key areas critical to effective program protection:

- ability to identify CPI;
- effectiveness in developing and implementing a program protection plan;
- training efforts for the protection of CPI;
- use of resources for the protection of CPI;
- effectiveness of policies to protect CPI;
- ability of counterintelligence, intelligence, and security to support the protection of CPI;
- effectiveness of the foreign visit program; and
- application of "horizontal protection" of CPI.

On December 12, 2008, the DoD Office of the Inspector General, Deputy Inspector General for Intelligence and the Deputy Under Secretary of Defense (Acquisition and Technology) cosigned a letter announcing the concept of this program protection assessment. The goal of the project was to conduct three assessments to evaluate how effectively DoD and each Military Department identify and protect CPI. The Warfighter Information Network – Tactical (WIN-T) is the first acquisition category (ACAT) ID[1] program of record assessed as part of the pilot. See Appendix A for a discussion of the scope and methodology.

---

[1] Acquisition Category I programs are major Defense acquisition programs. A major Defense acquisition program is a program estimated by the USD(AT&L) to require eventual expenditure for research, development, test, and evaluation of more than $365 million or procurement of more than $2.19 billion, or those designated by the USD(AT&L) to be major Defense acquisition programs or special interest programs. Acquisition category I programs have two subcategories: The first subcategory is ACAT IC, for which the milestone decision authority is the DoD Component Head or, if delegated, the Component Acquisition Executive. The second subcategory is ACAT ID, for which the milestone decision authority is the USD(AT&L). The Defense Acquisition Board advises the USD(AT&L) at major decision points. The USD(AT&L) designates programs as ACAT ID or ACAT IC.

Background

Warfighter Information Network – Tactical. WIN-T is a high-speed and high-capacity communications network designed to be the Army's tactical Internet. WIN-T is intended to provide reliable, secure, and seamless communications for theater and below initially to modular[2] brigade combat teams (and eventually to Future Combat Systems brigade combat teams). WIN-T is being developed and fielded in four increments that will build on one another:

- Increment 1 is the former Joint Network Node-Network program – stationary networking, which enables the exchange of voice, video, data, and imagery throughout the tactical battlefield using a satellite-based network;
- Increment 2 – networking on the move, provides command and control on the move down to the company level for maneuver brigades and implements the core network capability;
- Increment 3 – full networking on the move, provides full mobility command and control, to include Future Combat System support, for divisions and below; and
- Increment 4 – protected satellite communications on the move, includes access to the next generation of protected satellites while retaining all previous on the move capabilities.

Research and Technology Protection Oversight in the Army – The Army Inspector General and the Army Audit Agency. Through its Technical Inspections and Intelligence Oversight divisions, the Army Inspector General provides the Army's input to the annual summary report[3] of inspections on security, technology protection, and counterintelligence practices at research, development, test, and evaluation (RDT&E) facilities. The inspections focus on RDT&E facilities or installations with RDT&E tenants, including Government-owned, contractor-operated and contractor-owned, contractor-operated operations. The inspections check for compliance with Army guidance and identify for Army leadership ways to improve programs and facility security and disseminate best practices. By focusing on the inspection results, the Army Inspector General heightens awareness across the community and effectively addresses security vulnerabilities in Army laboratories and across all Army programs.

At the request of the Secretary of the Army, the Army Audit Agency audited the Army's research and technology protection (RTP) program, issuing five reports between May 2008 and April 2009. Neither the Warfighter Information Network -Tactical nor its program executive office was audited by the Army Audit Agency. However, the Army Audit Agency audits encompassed multiple locations and focused on the adequacy of procedures used to identify and protect CPI at Army program executive offices, a focus directly related to our assessment efforts.

---

[2] Modularity is a major restructuring of the entire Army, involving the creation of Brigade combat teams, from a Division-based force. The foundation of the modular force is the creation of standardized modular combat Brigades designed to be stand-alone, self-sufficient units that are more rapidly deployable and better able to conduct joint operations than divisions.

[3] Prepared by the DoD Office of the Inspector General, Office of the Deputy Inspector General for Intelligence, based on a request by the Deputy Secretary of Defense to ensure implementation of a uniform system of periodic reviews through the existing agency and Service inspection processes for compliance with directives concerning security, technology protection, and counterintelligence practices.

The Army Audit Agency stated that Army program executive offices had adequate procedures for identifying CPI; however, some improvements were needed in issuing guidance to program executive offices. OASA ALT - (b)(5)

[redacted] The Army Audit Agency also recommended issuing policies and procedures for providing protection guidance to users of end items with CPI, and having the working group being established to develop an Army regulation to implement DoD Instruction 5200.39 address the issues identified in the audit.

Criteria

DoD Policy and Implementation Guidance

It is DoD policy to provide uncompromised and secure military systems to the warfighter by performing comprehensive protection of CPI through the integrated and synchronized application of counterintelligence, intelligence, security, systems engineering, and other defensive countermeasures to mitigate risk. Failure to apply consistent protection of CPI may result in the loss of confidentiality, integrity, or availability of CPI, resulting in the impairment of the warfighter's capability and DoD's technological superiority. Additionally, it is DoD policy to mitigate the exploitation of CPI; extend the operational effectiveness of military systems through application of appropriate risk management strategies; employ the most effective protection measures, to include system assurance and anti-tamper; conduct comparative analysis of defense systems' technologies and in order that CPI protection is aligned horizontally throughout the DoD, document the measures in a program protection plan. Furthermore, DoD policy requires that contracts supporting RDA programs wherein CPI has been identified shall contain contractual terms requiring the contractor to protect the CPI to DoD standards.

DoD Instruction 5200.39 "Critical Program Information (CPI) Protection Within the Department of Defense," July 16, 2008 defines what constitutes CPI; establishes policy for the protection of CPI; and assigns responsibilities for counterintelligence, intelligence, security, and systems engineering support for the identification and protection of CPI. Furthermore, it details responsibilities relating to the identification of CPI and the implementation of program protection plans to DoD Components; and implements relevant parts of DoD Directive 5000.01, "The Defense Acquisition System," DoD Instruction 5000.02, "Operation of the Defense Acquisition System;" December 8, 2008, and continues to authorize the use of DoD 5200.1-M, "Acquisition Systems Protection Program," March 1994, to serve as implementation guidance. Also, DoD Instruction 5200.39 supplements existing policies and guidance related to the security of DoD personnel, information, resources, installations, and operations to include DoD contractors performing work or supporting DoD RDA efforts.

---

[4] Horizontal protection ensures that critical Defense technologies, including critical program information, associated with more than one RDA program are protected to the same degree by all involved DoD activities. It is DoD policy to conduct comparative analysis of Defense systems technologies and align critical program information protection activities horizontally throughout DoD.

DoD Instruction 5000.02 "Operation of the Defense Acquisition System," December 8, 2008 establishes within DoD acquisition policy that during the technology development phase that the technology development strategy shall document a listing of CPI and potential countermeasures, such as anti-tamper, in order to inform program protection planning and design integration. Further, CPI shall be identified as early as possible, and shall inform the preparation of the program protection plan. Additionally, during the engineering and manufacturing development phase it states that the protection of CPI is implemented by applying appropriate system engineering and security techniques, such as anti-tamper. Moreover, DoD Instruction 5000.02, Enclosure 4 details "Statutory and Regulatory Information and Milestone Requirements" that apply to all acquisition programs; and details each milestone and decision point setting forth mandatory requirements relevant to the identification and protection of CPI.

DoD 5200.1-M "Acquisition Systems Protection Program," March 1994 prescribes standards, criteria, and methodology for the identification and protection of CPI (described as Essential Program Information, Technologies, and/or Systems within this Manual) within DoD acquisition programs. The protection standards and guidance described within this Manual are required to prevent foreign intelligence collection and unauthorized disclosure of essential program information, technologies and/or systems during the DoD acquisition process.

Defense Acquisition Guidebook, Chapter 8, "Intelligence, Counterintelligence, and Security Support," addresses actions required once CPI is identified within an acquisition program and identifies the critical elements in a comprehensive acquisition protection strategy, including:

- the responsibilities of program managers (PM) in the prevention of inadvertent transfers of dual-use and leading-edge military technologies used in defense platforms;
- the availability of intelligence, counterintelligence, and security support for acquisition programs and the requirement to use them; and
- guidance and descriptions of support available for protecting technologies.

Army Policy and Implementation Guidance

Army Regulation 70-1, "Army Acquisition Policy," December 31, 2003 implements DoD Directive 5000.1, DoD Instruction 5000.2, and governs RDA and life-cycle management of Army materiel within Army acquisition programs. This regulation is the first order of precedence for managing Army acquisition programs following the Federal Acquisition Regulation, Defense Federal Acquisition Regulation Supplement, DoD regulation direction and Army Federal Acquisition Regulation Supplement. It assigns responsibility for security, intelligence, and counterintelligence, policy for the Army's acquisition process and for security, intelligence and counterintelligence support to Army acquisition programs with CPI.

Department of the Army Pamphlet 70-3, "Army Acquisition Procedures," January 28, 2008 provides guidance on materiel acquisition management and is used in conjunction with DoD Directive 5000.01, DoD Instruction 5000.02, and Army Regulation 70-1. It contains information relevant to RDA and life-cycle management of Army materiel to satisfy approved Army requirements. It details timelines and procedures for CPI identification, the development of a program protection plan, and obtaining threat products. Additionally, it provides guidelines for information security involving controlled unclassified information to foreign entities.

Army Regulation 380-10, "Foreign Disclosure and Contacts With Foreign Representatives," June 22, 2005 implements the national policy and procedures for the disclosure of classified military information to foreign governments and international organizations, as detailed in DoD Directives 5230.11 and 5230.20 and in DoD Instruction 2040-02.[5] The regulation addresses three areas:

- general disclosure policies, the authority to disclose, and the delegation of authority;
- modes, methods, and channels for disclosures of classified military information; and
- the Army's technology protection program.

Relative to CPI, the regulation details the establishment and composition of a technology control panel to review and develop policy related to the Army's critical technologies.

Army Regulation 381-11, "Intelligence Support to Capability Development," January 26, 2007 provides policies, responsibilities, and procedures to ensure that threat considerations are incorporated into the Defense acquisition process and the Joint Capabilities Integration and Development System. The regulation provides detailed implementation of intelligence activities that support CPI identification; the development of threat products, i.e. System Threat Assessment Report, Multidisciplinary Counterintelligence Threat Assessment, that support research and technology protection, and foreign disclosure determinations.

Summary of Report

We organized the results of this assessment into two findings. Finding A discusses the policies and structure of the Army to protect CPI and details how the Army's efforts to protect CPI could be strengthened to better protect Army research and technology programs and activities across the Army. In Finding B, we use WIN-T as a case study to assess the eight issue areas. We address each issue area separately, focusing on standardization of protection processes and their application, oversight of the protection processes, and responsibility for the protection. We assess whether the published guidance on the protection of CPI in each issue area was relevant and whether program, intelligence, counterintelligence, and security personnel adhered to the guidance. In those instances where efforts to protect CPI could be strengthened, we make recommendations for improvements. We also note best practices.

---

[5] DoD Directive 5230.11, "Disclosure of Classified Military Information to Government and International Organizations, June 16, 1992; DoD Directive 5230.20, "Visits and Assignments of Foreign Nationals," June 22, 2005; and DoD Instruction 2040.02, "International Transfers of Technology, Articles and Services," July 10, 2008.

Finding A. Army Policy and Structure Need Improved Integration for Maximum Protection of Critical Program Information

Current research and technology protection (RTP) efforts of the Army do not provide the most efficient and comprehensive technology protection. The three key participants in the Army's RTP process are the Assistant Secretary of the Army (Acquisition, Logistics, and Technology) (ASA)ALT); the Commanding General, Army Materiel Command; and the Deputy Chief of Staff, G-2 (Intelligence); however, their efforts are not integrated and synchronized to the greatest extent possible, and they are not optimizing the ability to provide standardized efforts to protect Army research and technology programs or activities across the Army.

Policies Establishing Roles for Research and Technology Protection

DoD and the Army continually seek ways to deal with the complexities of program protection because synchronization across so many commands and functional areas is a challenge.

Department of Defense Policy

DoD Instruction 5200.39 establishes the responsibilities of the Under Secretary of Defense (Acquisition, Technology, and Logistics) (USD(AT&L)) for the protection of CPI in DoD acquisition programs. It instructs the USD(AT&L) to lead in the establishment of a consistent process for the identification and protection of CPI and to require a program protection plan[6] for RDA programs in which CPI has been identified.

As the milestone decision authority for major defense acquisition programs, the USD(AT&L) also has the lead in establishing procedures outlining program protection plan development and approval in collaboration with the Under Secretary of Defense (Intelligence), the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer, the Under Secretary of Defense (Policy), and with DoD Components.

---

[6] The program protection plan is designed as a dynamic planning tool to capture in a single document the most effective means to protect CPI from unauthorized foreign collection activities and unauthorized disclosure; and to develop those protection measures that will ensure a combat system's effectiveness throughout its lifecycle. When a determination of CPI is made, a program protection plan is required for milestone decision authority review and approval at all milestones. The program protection plan is required to address the foreign collection threat to the CPI that has been identified by intelligence and counterintelligence agencies. Within the Army, the PM is required to develop the program protection plan. To this end, the PM is supported by the Deputy Chief of Staff, G-2's Army Research and Technology Protection Center, and the Army Materiel Command, G-2. Based upon the identification of CPI, the PM obtains validated threat products from the Army Counterintelligence Center, and the system threat assessment from the National Ground Intelligence Center in order to develop credible, cost effective system engineered security and countermeasures.

In addition, DoD Instruction 5200.39 authorizes the USD(AT&L) to provide direction and management oversight for the identification and protection of CPI for programs under the cognizance of the USD(AT&L).

Army Policy

To implement the requirements to protect CPI, Army Regulation 70-1[7] established an Army Research and Technology Protection Center (ARTPC) under the auspices of the Deputy Chief of Staff, G-2. The ARTPC was created to support acquisition programs over which the Army has cognizance by integrating and synchronizing security, intelligence, counterintelligence, foreign disclosure, and security countermeasure support to RTP activities Army-wide.

Army Regulation 381-11 tasks the ASA(ALT) to ensure that there are sufficient intelligence resources to support long-range planning and that plans reflect the threat. Army Regulation 381-11 also requires the ASA(ALT) to obtain and fund multidisciplinary intelligence support for RDA requirements. As the Army Acquisition Executive, the ASA(ALT) serves as the milestone decision authority for major Army acquisition programs and has approval authority for corresponding acquisition program protection plans.

Army Regulation 381-11 requires the Army Materiel Command to determine intelligence support requirements for threats to capability development under Army Materiel Command purview and to provide requisite threat support in collaboration with other threat support activities and the Deputy Chief of Staff, G-2; provide foreign intelligence officers at the appropriate Life Cycle Management Commands, Research, Development, and Engineering Commands, and laboratories to serve as the primary sources of multidisciplinary intelligence support to program executive offices/PMs and technical and laboratory directors; coordinate with program executive offices/PMs and the Deputy Chief of Staff, G-2, to ensure appropriate funding is provided for multidisciplinary intelligence support of Army RDA programs; serve as the Army point of contact for coordination of input to the military critical technology list; provide multidisciplinary intelligence support and guidance to technology-based programs; and provide threat input to program management documents.

Where intelligence gaps exist, the Regulation requires the Army Materiel Command to prepare and submit requirements for new intelligence; provide technology assessments in support of international cooperative programs, foreign comparative testing, technology protection, and export control activities; and identify and submit command intelligence support requirements.

---

[7] At the time Army Regulation 70-1 was published, DoD Directive 5200.39, "Security, Intelligence, and Counterintelligence Support to Acquisition Program Protection," September 10, 1997 was the existing guidance for the protection of CPI; however, DoD Instruction 5200.39 was published in 2008 and provides the current guidance for the protection of CPI.

The Army's Research and Technology Protection Program

The Army's RTP program was established to provide tailored, life-cycle comprehensive RTP to DoD acquisition programs with CPI, and to Research, Development, and Engineering Centers where critical research is conducted. The acquisition, security, intelligence, and counterintelligence communities work together to develop an integrated approach to protecting the sophisticated technology in Defense systems.

Under this program, the ASA(ALT) has overall responsibility for protection of research and technology. To support these protection efforts, the Army Materiel Command has life-cycle protection responsibilities; and the Deputy Chief of Staff, G-2, provides security, intelligence, and counterintelligence support.

The ASA(ALT), in conjunction with representatives from the Army Materiel Command and the Deputy Chief of Staff, G-2, is developing RTP policy for the Army. The ASA(ALT) anticipates that the policy will be completed by December 15, 2010.

Players and Roles

Army's Defense Industrial Base[8] Cyber Security Office

The Army Defense Industrial Base Cyber Security Office, formerly the Army Defense Industrial Base Cyber Security Task Force, was created in the ASA(ALT) to address two key trends facing program protection in the defense industrial base: (1) digitalization of information and (2) globalization of economic activity.

- Digitalization of information has introduced greater risk of compromise of DoD-controlled unclassified information, held by the defense industrial base, that is used in the development of warfighting systems during the acquisition life cycle.
- OASA ALT - (b)(4) [redacted]
- OASA ALT - (b)(4) [redacted]
- OASA ALT - (b)(4) [redacted]

These trends necessitate a much more comprehensive approach to acquisition risk management than has traditionally been taken.

---

[8] The defense industrial base includes hundreds of thousands of domestic and foreign entities and their subcontractors performing work for DoD and other Federal agencies. Defense-related products and services provided by the defense industrial base equip, inform, mobilize, deploy, and sustain forces conducting military operations.

OASA ALT - (b)(4)

[redacted]. DoD Instruction 5200.39 clarifies definitions, responsibilities, and roles for protecting CPI.

Because no single office existed within the Army to manage these and other emerging risks, the ASA(ALT) created the Defense Industrial Base Cyber Security Office, which is responsible for organizing and coordinating Army efforts to mitigate risks to Army acquisition programs. The Defense Industrial Base Cyber Security Office focuses on countering cyber extraction of controlled unclassified information from defense industrial base unclassified networks. For more information on the Army Defense Industrial Base Cyber Security Office, see Appendix E.

Army Materiel Command

The Army Materiel Command is the Army's principal materiel developer and is the Army's Executive Agent for RTP across the materiel lifecycle. In the Army's 2009 campaign plan, the Army Materiel Command was tasked to, in conjunction with the ASA(ALT) and the Training and Doctrine Command, develop and field advanced technology to provide materiel solutions to the current and future forces and to establish safeguards for newly developed and existing technologies through effective technology protection programs.

The mission of the Army Materiel Command, G-2 (Intelligence) is to protect sensitive programs and information, identify threats to current capabilities and technologies under development, and provide intelligence and security support to Army Materiel Command strategic plans and operations.

The mission of the Army Materiel Command, G-2's Technology Protection Division is to identify and protect CPI from the earliest point possible to mitigate the risk of compromise. This is accomplished through developing, implementing and overseeing policies and programs to ensure their relevance and effectiveness throughout the commands; through ensuring that the research and technology program is mainstreamed by the RDA community; and through providing comprehensive counterintelligence support to Army Materiel Command requirements.

The Army Materiel Command also has a Technology Protection Officer located at four Life Cycle Management Commands to provide expert, authoritative, multidisciplinary security, program protection, and policy advice; conduct multidisciplinary protection planning of weapons systems, programs, and projects; and provide life-cycle protection support to pre-acquisition and acquisition programs, whether in development or fielded. The technology protection officer conducts in-depth technology assessments and system decomposition of RDT&E and acquisition programs to identify CPI.

The Technology Protection Officer orchestrates and synchronizes program protection support activities, including security, program protection, program protection training, classification management, industrial security, operations security, public affairs, system security engineering, threat data requirements, counterintelligence, technical intelligence, foreign disclosure, anti-tamper measures, and technology transition.

The Technology Protection Officer integrates requirements for threat intelligence, risk assessments, vulnerability analysis, program protection plans, technology control plans, and countermeasure implementation. The Technology Protection Officer also manages issues such as national disclosure policy, foreign relations, commercial and dual-use commodities, and export controls.

During our on site visit to talk with WIN-T program, CECOM Life Cycle Management Command, counterintelligence, and Defense Security Service[9] officials, the technology protection officer had relocated to Aberdeen Proving Ground, MD, we discovered that the Technology Protection Officer was also not represented on the WIN-T integrated product team process.

The Army Deputy Chief of Staff, G-2/and the Army Research and Technology Protection Center

The concept of the ARTPC, under the Deputy Chief of Staff, G-2, evolved in August 2000, when the Chief of Staff of the Army asked "How will we ensure when we field FCS [Future Combat System]/Objective Force that the technological overmatch designed-in is protected?" That question was the impetus for an assessment of how the Army protects research and technology. The assessment identified the following protection obstacles and deficiencies.

- Accountable officials lacked knowledge about protection planning.
- Policies were parochial, ambiguous, or contradictory.
- Consistency in meeting protection requirements was lacking.
- No standard of sufficiency existed, leading to overprotection or underprotection.

In response, the Army sought to establish a consistent process and standard for technology protection by:

- providing full-time, skilled technology protection support;
- assigning Technology Protection Engineers to acquisition nodes;
- providing onsite or "on request" support to PMs;
- integrating and coordinating technology protection efforts of others;
- continuing mission area analysis to enable continuous improvement; and
- assembling functional experts in program protection, threat management, foreign disclosure, security, vulnerability, and policy; Technology Protection Engineers;[10] and program protection architects;[11]

---

[9] The Defense Security Service: assists DoD Component counterintelligence elements in coordinating the execution of a counterintelligence support plan at cleared Defense contractors with CPI; develops and conducts training for DoD and Defense contractor security personnel regarding CPI protection activities; and during the conduct of regularly scheduled security inspections at cleared Defense contractor facilities, determine if there are any contractually imposed protection measures for CPI related to classified contracts at these locations.

[10] Technology protection engineers have the following types of technical education and experience: electrical engineering, mechanical engineering, industrial engineering, system security engineering, software engineering, aeronautical engineering, nuclear engineering, information technology, physics, and chemistry.

[11] Program protection architects have the following types of technical education and experiences: security, intelligence, and law enforcement backgrounds; program protection, information security, information

To establish consistency and to standardize CPI identification and protection Army-wide, the ARTPC was established by the Deputy Chief of Staff, G-2 in October 2002. The ARTPC's purpose is to ensure that the RTP planning process achieves the goal of protecting the Army's CPI. The ASA(ALT) issued a memorandum that encourages Army acquisition programs to use the ARTPC in identifying CPI in their programs. In its efforts to support Army RTP efforts, the ARTPC has adopted a 360-degree protection approach, consisting of:

- security classification guides,
- delegation of disclosure authority letters,
- a communications strategy,
- contracts,
- patents,
- operations (including testing),
- operations security,
- CPI identification,
- program protection plans, and
- technology protection plans.

The ARTPC takes a best practice approach in composing its RTP teams. It integrates technologists, engineers, and security experts to assist in the two most important aspects of RTP: identification of CPI, and implementation of countermeasures to protect CPI. That the ARTPC has engineers and technologists who are trained in counterintelligence and security, as opposed to counterintelligence and security professionals who receive training in engineering and technologies, helps them better understand cutting-edge technologies and the threats to those technologies – especially in developing and implementing countermeasures to counter these threats as early in the process as possible.

Areas to Improve Integration, Synchronization, and Optimization for Maximum Protection of Critical Program Information

To highlight where the program protection structure is uneven, the Deputy Chief of Staff, G-2's ARTPC has a good blend of technical and program security professionals; however, their role is limited to the facilitation of CPI identification and corresponding countermeasure development.

The Army Material Command has life-cycle CPI protection responsibilities, but the technology protection officer was not integrated into the WIN-T integrated product team process, and although the Program Executive Office for Command, Control, Communications Tactical has comprehensive program protection plan implementation guidance, the list of program protection team representation does not include the technology protection officer. The Army Materiel Command's life-cycle protection efforts would be enhanced by being involved in all aspects of program protection, especially sustainment and demilitarization.

---

assurance, classification management, physical security, operations security, counterintelligence threat analysis, counterintelligence operations, human intelligence, law enforcement, special access program security, personnel security, foreign disclosure policy, industrial security, anti-terrorism, threat analysis, tactical intelligence, operational intelligence, strategic intelligence, and asset protection.

Above all, the ASA(ALT), primarily through its program executive offices and PMs, has responsibility for all aspects of program execution, to include security. By ensuring program executive offices and PMs are cognizant of standardized protection processes and their application, overseeing the protection processes, and knowing their responsibility for and leveraging protection efforts, it will greatly support the program goals of cost, schedule, and performance when making security-related decisions, such as the application of countermeasures like anti-tamper, the associated costs, and the subsequent effectiveness of those countermeasures.

Although the above policies highlight the different roles and responsibilities for the Army to protect its CPI, the policies do not focus on total integration of security, intelligence, and counterintelligence throughout a program's lifecycle. In its April 29, 2009 report "Army Research and Technology Protection Program: Office of the Assistant Secretary of the Army (Acquisition, Logistics, and Technology)," Audit Report No. A-2009-0094-ZBI, the Army Audit Agency recommended that the ASA(ALT) issue guidance to program executives to: document determinations that systems do not contain CPI; obtain protection guidance from other programs that provide items with CPI; assign responsibility for implementing program protection plans; ensure that statements of work clearly describe the requirements for contractors to implement program protection plans; develop a tracking system to monitor the implementation status of countermeasures; develop and issue policy and procedures for providing protection guidance to users of end items with CPI; and [most importantly] ensure that the working group being established to develop an Army regulation to implement DoD Instruction 5200.39 address the issues identified in the audit. The ASA(ALT) agreed and is in the process of implementing the recommendations.

As the lead for developing RTP policy for the Army, the ASA(ALT), in conjunction with the Army Materiel Command, and the Deputy Chief of Staff, G-2 can ensure that the Army's new RTP policy standardizes RTP efforts, as well as clearly delineate responsibilities to integrate, synchronize, and optimize Army cradle-to-grave efforts to protect CPI. The ASA(ALT), through this process, can also ensure that Army efforts to protect CPI are closely aligned with DoD efforts and guidance.

Conclusion

Protection activities span Military Departments, DoD agencies, and beyond, coordination and integration of RTP requires Department-level emphasis and involvement. Aligning Army RTP efforts with ongoing DoD RTP efforts, as outlined in DoD Instruction 5200.39, will allow greater integration and synchronization across the Army and DoD. Policy, training, and oversight should be synchronized to allow the most effective use of RTP personnel and to ensure proper execution of program protection plans, from concept to demilitarization.

Additionally, the ASA(ALT) appoints the PM, who is responsible for all aspects of program execution, including its security. As the central participant for program protection, the PM should have a complete understanding of the capabilities that the security, intelligence, and counterintelligence communities can provide.

Because the ARTPC takes a best practice approach in the formulation of its RTP teams, it greatly enhances the teams' ability to provide assistance in the two most important aspects of RTP – identification of CPI and implementation of countermeasures to protect CPI.

Integrated product teams could benefit immeasurably from the unique perspective of the ARTPC. The ARTPC concept is also integral to any command's functions for executing RTP: integration and synchronization of CPI countermeasures from cradle to grave.

As the Army's materiel developer, the Army Materiel Command has responsibility for RTP support to all Army organizations executing RDA across the materiel lifecycle. Moreover, with the dedicated RTP support provided by the ARTPC and the Army Materiel Command, G-2, specifically with the Technology Protection Engineers and technology protection officers, the PM could ensure that they are optimizing the available RTP support to the greatest extent possible. However, this does not occur in a concerted and deliberate manner. The ASA(ALT), Army Materiel Command, and Deputy Chief of Staff, G-2 must ensure that their RTP efforts, policy, and training are integrated, synchronized and optimized, and are aligned with DoD efforts.

Recommendations, Management Comments, and Our Response

A. We recommend that the Assistant Secretary of the Army for Acquisition, Logistics, and Technology, in conjunction with the Commanding General, Army Materiel Command, and the Army Deputy Chief of Staff, G-2, review and develop a plan of action that will result in the most efficient and effective means to integrate, synchronize, and optimize research and technology protection efforts for the Army.

Management Comments

On behalf of the Commanding General, Army Materiel Command and the Army Deputy Chief of Staff, G-2, the Assistant Secretary of the Army for Acquisition, Logistics, and Technology concurred with the recommendation. The Assistant Secretary of the Army for Acquisition, Logistics, and Technology, with input from the Army Deputy Chief of Staff, G-2, the Army Research and Technology Protection Center, and the Army Materiel Command G-2 are developing an Army regulation that will address research and technology protection responsibilities to ensure Army programs properly identify critical program information and implement countermeasures to effectively prevent compromise of critical program information. The Assistant Secretary of the Army for Acquisition, Logistics, and Technology expects to publish the regulation by December 15, 2010.

Our Response

The consolidated comments of the Assistant Secretary of the Army for Acquisition, Logistics, and Technology, the Commanding General, Army Materiel Command, and the Army Deputy Chief of Staff, G-2 are responsive and meet the intent of the recommendation. Please provide us a draft of the regulation prior to issuance.

Finding B. The Army's Warfighter Information Network – Tactical Program's Efforts to Protect Critical Program Information

Within the framework of the eight issue areas, we assessed program protection efforts for standardization of CPI protection processes and their application, oversight of the CPI protection process and its implementation, and responsibility for the protection of CPI, using the Army's WIN-T as a program of record case study. Recent DoD issuances, such as DoD Instruction 5200.39, were the primary assessment tool for this pilot and have established a good framework for RTP. However, and in spite of demonstrated best practices, efforts are not fully integrated, synchronized, and optimized to the greatest extent possible and do not provide standardized efforts to protect CPI across the Department. We found the following:

- Areas of existing issuances need to be enhanced; new guidance needs to be crafted, such as guidance for anti-tamper measures; and the DoD CPI protection manual containing detailed measures for RTP should be promulgated.
- Guidance should be established for identifying commercial off-the-shelf/government off-the-shelf components as critical program information, to include assessment tools and training.
- Standardized guidance for training in CPI protection should be developed for use by the RTP community.
- Guidance should be provided on model contract language in support of program protection planning to DoD and Component RTP officials.
- Guidance should be developed that describes:
    - what can and should be contained in the DD Form 254, "Department of Defense Contract Security Classification Specification," for the protection of controlled unclassified CPI,
    - how program protection should be implemented at the level of subcontractors, and how to verify contractor compliance with the DD Form 254 and the program protection plan
- Security requirements for contractors processing CPI on non-DoD information systems should be developed and published.
- The appropriateness of using the Secret Internet Protocol Router network as the host for the horizontal protection database should be determined.

Issue Area One: Ability to Identify Critical Program Information

We assessed this issue area to determine whether published guidance for the identification of CPI is relevant to and adhered to by program, security, intelligence, and counterintelligence personnel. We also sought to determine whether there was a working-level integrated product team to assist with and collaborate on the identification of CPI. If so, we wanted to assess how the mission, composition, and effectiveness of the working-level integrated product team contributed to the identification of CPI and whether the working-level integrated product team performed a functional decomposition of the program or system. We determined that the WIN-T program office had an effective process for identifying CPI.

DoD Instruction 5200.39 states that the USD(AT&L) should:

- lead the effort, in collaboration with the Under Secretary of Defense (Intelligence) and the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer, to establish a consistent process for the identification and protection of CPI that takes into account the role that research, development, acquisition, counterintelligence, intelligence, security, and systems engineering personnel perform;
- provide direction and management oversight for the identification and protection of CPI for RDA programs under the cognizance or oversight of the USD(AT&L);

Because of the current definition of CPI in DoD Instruction 5200.39, guidance that clarifies that CPI can be either critical technology or functionality, WIN-T did not identify CPI at the outset, but recently identified CPI in its latest CPI identification integrated product team process.

Warfighter Information Network – Tactical Integrated Product Team. WIN-T program management office personnel, serving on an integrated product team with representatives from the ARTPC, prime and subcontractors, the National Ground Intelligence Center, and 902nd Military Intelligence Group,[12] conducted a CPI assessment of the WIN-T Increments 2 and 3 beginning January 20 and ending January 29, 2009. The team comprised systems engineering, information assurance, engineering management, and software engineering experts. We did not find that science and technology expertise was represented on the team. The ARTPC facilitated the process, focusing on the WIN-T network's functionality and architecture and on the design modifications required to implement the WIN-T network integration of commercial off-the-shelf, Government off-the-shelf, and custom items. The integrated product team assessed all items configured under WIN-T Increments 2 and 3, using the ARTPC CPI tool.[13]

On February 11, 2009, the Acting ASA(ALT) published a memorandum, "Identification and Protection of Critical Program Information (CPI)," stating that PMs will use integrated product teams comprising program, technical, systems engineering, counterintelligence, intelligence, and security experts to assist in identifying CPI.

The WIN-T program used a cross-discipline integrated product team that included systems engineers, demonstrating that the DoD Instruction 5200.39 requirement for cross-discipline teams is already proving effective. However, the reason for lack of science and technology participation should be explored and rectified, either through clarification in the forthcoming program protection manual or through training or guidance.

---

[12] The 902nd Military Intelligence Group and National Ground Intelligence Center are elements of the U.S. Army Intelligence and Security Command, which, along with the ARTPC, are elements of the U.S. Army Deputy Chief of Staff for Intelligence (G-2).

[13] The ARTPC tool is a survey tool that guides the user through a series of questions to ascertain whether the program potentially contains critical program information.

Warfighter Information Network – Tactical and Anti-tamper. The March 2004 Government Accountability Office Report, "DoD Needs to Better Support Program Managers' Implementation of Anti-Tamper Protection," identified defining critical technology as the first step and the basis for determining the need for anti-tamper[14] countermeasures. The anti-tamper section of Chapter 8 of the Defense Acquisition Guidebook states that PMs should develop and implement anti-tamper measures to protect CPI in U.S. defense systems developed using co-development agreements; sold to foreign governments; or removed from U.S. control through theft or battle loss. OASA ALT - (b) (5)

[redacted]

OASA ALT - (b)(5)

[redacted]

In its January 2008 report "Departmentwide Direction is Needed for Implementation of Anti-Tamper Policy," the Government Accountability Office recommended that" the Secretary of Defense direct the Under Secretary of Defense (Acquisition, Technology, and Logistics), in coordination with the Anti-Tamper Executive Agent and the Under Secretary of Defense (Intelligence), to issue department-wide direction for application of its anti-tamper policy that prescribes how to carry out the policy and establishes definitions for critical program information and critical technologies."

In its response DoD non-concurred, stating that "The USD(I) is the office of primary responsibility for DoDD[irective] 5200.39, "Security, Intelligence and Counterintelligence Support to Acquisition Program Protection," and its successor, DoDI[nstruction] 5200.39, "Critical Program Information (CPI) Protection within the Department of Defense." USD(I) is currently coordinating an update to the directive. The Anti-Tamper Executive Agent has proposed the incorporation of anti-tamper policy in this revision. The considered policy for anti-tamper mandates: "For critical technology type CPI, employ appropriate anti-tamper during the RDA process unless waived in writing by MDA or equivalent." Following the issuance of the updated DoDI 5200.39, the Department will revise the DoD 5200.1-M, "Acquisition Systems Protection," the implementing manual for the directive which provides the execution standards and guidelines to meet the DoDI 5200.39 policy. The Anti-Tamper Executive Agent's plan is to include a new section in the manual that is explicitly for anti-tamper. This will describe how to implement anti-tamper to protect technology CPI for U.S.-only cases, foreign military sales/direct commercial sales, and science and technology programs."

---

[14] Anti-tamper measures refer to the systems engineering activities intended to prevent or delay exploitation of critical technologies in U.S. weapons systems. These activities involve the entire lifecycle of systems acquisition, including research, design, development, implementation, and testing of anti-tamper measures.

However, DoD Instruction 5200.39 was published in 2008 with little OASA ALT (b)(5) guidance. OASA ALT (b)(5) The Defense Acquisition Guidebook does provide some information on OASA ALT (b) (5) .

Warfighter Information Network - Tactical and Commercial Off-the-Shelf/Government Off-the-Shelf

Another issue was commercial off-the-shelf components as CPI candidates. No guidance on commercial off-the-shelf components and corresponding protection mechanisms appears in DoD Instruction 5200.39 or in chapter eight of the Defense Acquisition Guidebook. Critical program information assessment tools, guidance, and training should be reviewed, and modifications should be considered to address identification of commercial off-the-shelf components as CPI.

The guidance should allow the possibility that commercial off-the-shelf components are CPI or that the commercial off-the-shelf components' functionality is so critical to the CPI functionality that the countermeasure (for example, anti-tamper packaging or supply chain risk mitigation) is best applied to the commercial off-the-shelf component.

The USD(AT&L) and the Under Secretary of Defense (Intelligence) are leading working groups (see Appendix D) on initiatives to improve the protection of CPI and develop a standardized process for identifying CPI and associated countermeasures, to include anti-tamper. In addition, the Under Secretary of Defense (Intelligence) is leading efforts to ensure a CPI identification tool is being incorporated in a forthcoming CPI protection manual. Standardizing the process for identifying CPI will ultimately minimize subjectivity.

Conclusion

WIN-T program office staff had an effective process for identifying CPI. The process used an integrated product team and the ARTPC. The USD(AT&L) and the Under Secretary of Defense (Intelligence) are leading working groups (see Appendix D) formed to improve the protection of CPI by, among other things, developing a standardized process for identifying CPI.

OASA ALT - (b)(5)

Critical program information assessment tools, guidance, and training should be reviewed, and modifications should be considered, to address identification of commercial off-the-shelf components as CPI. The guidance should allow the possibility that commercial off-the-shelf components are CPI or that the commercial off-the-shelf component's functionality is so critical to the CPI functionality that the countermeasure (for example, anti-tamper packaging or supply chain risk mitigation) is best applied to the commercial off-the-shelf component.

Recommendations, Management Comments, and Our Response

B1-1. We recommend that the Under Secretary of Defense for Acquisition, Technology, and Logistics, in consultation with the Under Secretary of Defense for Intelligence, the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer, and Component RTP officials promulgate anti-tamper policy that ensures that anti-tamper countermeasures are considered early in the identification process, are standardized, and can be integrated throughout the Department.

Management Comments

The Under Secretary of Defense for Acquisition, Technology, and Logistics, the Under Secretary of Defense for Intelligence, and the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer concurred with the recommendation to [redacted]

OASA ALT - (b)(5)

Our Response

The comments of the Under Secretary of Defense for Acquisition, Technology, and Logistics, the Under Secretary of Defense for Intelligence, and the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer are partially responsive in meeting the intent of the recommendation. Although the draft DoD Manual 5200.39-M, "Procedures for Critical Program Information Protection Within the Department of Defense," is in the formal coordination stage, throughout this report organizations make reference to the draft manual as containing the resolution to our recommendations. As the proponent for the manual, the Under Secretary of Defense for Intelligence should provide a date when the draft manual will be completed. Additionally, if the Under Secretary of Defense for Acquisition, Technology, and Logistics believes that the formal coordination process for the draft manual will prevent timely guidance from reaching program protection officials, then steps should be taken to provide interim guidance, such as a policy letter or directive type memorandum, to ensure timely delivery of anti-tamper guidance. Guidance that provides consistency across the Department and ensures anti-tamper is considered early will also save money by alleviating the need to pay for costly anti-tamper countermeasures later in the program's development.

B1-2. We recommend that the Under Secretary of Defense for Acquisition, Technology, and Logistics establish guidance for identifying commercial off-the-shelf/government off-the-shelf components as critical program information, to include assessment tools and training efforts.

Management Comments

The Under Secretary of Defense for Acquisition, Technology, and Logistics concurred with the recommendation.

Our Response

The comments of the Under Secretary of Defense for Acquisition, Technology, and Logistics are partially responsive in meeting the intent of the recommendation. The Under Secretary of Defense for Acquisition, Technology, and Logistics should provide an action plan and a date for establishing the guidance for identifying commercial off-the-shelf/government off-the-shelf components as critical program information, to include assessment tools and associated training efforts.

Issue Area Two: Effectiveness in Developing and Implementing a Program Protection Plan

We assessed this area to determine whether published guidance for the planning of program protection is relevant and adhered to by program, intelligence, counterintelligence, and security personnel and to ensure that program protection planning was in accordance with DoD Instruction 5200.39. Because the WIN-T program office had not completed its program protection plan; we are unable to assess the plans effectiveness.

DoD Instruction 5200.39 states that it is DoD policy to require that contracts supporting RDA programs where CPI has been identified contain language requiring the contractor to protect the CPI to DoD standards. DoD Instruction 5200.39 also states that the USD(AT&L) should:

- require a program protection plan for all RDA programs with CPI within the purview of the USD(AT&L) and establish procedures outlining the program protection plan development and approval process in coordination with the Under Secretary of Defense (Intelligence), the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer, the Under Secretary of Defense (Policy), and the DoD Components; and
- lead the collaboration with the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer and the DoD Components for review of major Defense acquisition programs' program protection plans for sufficiency before their Defense Acquisition Board milestone decision reviews and at major acquisition strategy updates.

The program protection plan is used to develop tailored protection guidance for dissemination and implementation throughout the program for which it is created. The layering and integration of the selected protection requirements documented in a program protection plan provide for the integration and synchronization of CPI protection activities. The following are considered key elements of a program protection plan and are tailored to meet the requirements of a RDA program:

- technology and project description or system and program description, with an emphasis on what is unique, as the foundation for identifying CPI;
- list of CPI to be protected in the program (this generally describes classified CPI in an unclassified manner and is not suitable for horizontal protection analysis or the preparation of a counterintelligence assessment);
- threats to CPI;
- foreign threats;
- a summary of the counterintelligence assessment (the full report is an attachment to the plan);
- vulnerabilities of CPI to identified threats;
- countermeasures (all disciplines, as appropriate);
- counterintelligence support plan;
- anti-tamper annex;
- operations security plan;
- system assurance;
- technology assessment/control plan;

- classification guides;
- protection costs; and
- follow-on support.

The February 11, 2009 memorandum, "Identification and Protection of Critical Program Information (CPI)," published by the Acting ASA(ALT), states that program management offices should seek the services offered by the ARTPC in developing protection countermeasures.

OASA ALT - (b)(5)

[redacted]

OASA ALT - (b)(5)

[redacted]

We recommend the Army Audit Agency's April 29, 2009 report "Army Research and Technology Protection Program: Office of the Assistant Secretary of the Army (Acquisition, Logistics, and Technology)," Audit Report No. A-2009-0094-ZBI, to program office personnel.

OASA ALT - (b)(5)

[redacted]

In addition, and is written in the Program Executive Office Command, Control, Communications Tactical's Program Protection Plan policy and implementation guidance, the

OASA ALT - (b)(4), (b)(5)

[redacted]

[redacted]

Publishing guidance that provides model contract language would make it easier for programs to contract for CPI protection. Program management offices should do the following:

- provide the Defense Security Service with the program protection plan and the program office's specific requirements for the cleared contractor and the related documents for the protection of CPI, a list of the related counterintelligence and security risks to the contractor, and a copy of the relevant counterintelligence support plan;
- ensure that contracts require the prime contractor to participate in the identification of CPI and to implement countermeasures for identified CPI at contractor facilities;
- ensure contracts and DD Forms 254 include clauses authorizing certain Government personnel access to prime contractor and subcontractor facilities to conduct surveys, assessments, inspections, and investigations as necessary to make sure CPI is properly protected; and
- include language in contracts that the prime contractor must:
  - communicate program protection requirements to subcontractors that will have access to or will be providing CPI,
  - require subcontractors to continually monitor protection measures, and
  - monitor the subcontractors' performance monitoring.

Conclusion

Once the WIN-T program protection plan is complete, and as outlined in the Army Audit Agency reports and Program Executive Office Command, Control, Communications Tactical's Program Protection Plan policy and implementation guidance, the WIN-T PM should fully implement countermeasures articulated in the program protection plan, meeting specific milestone dates for their implementation; develop a tracking system for monitoring the implementation of the countermeasures; conduct site visits to assess the contractor's implementation of the countermeasures; and use the results of the site visits to evaluate the effectiveness of the countermeasures. The WIN-T PM should also require the contractor to prepare a program protection implementation plan to inform the WIN-T program management office how the contractor intends to protect CPI and implement the countermeasures articulated in the program protection plan. Providing contract language in guidance would make it easier for the program management office to contract for CPI protection. Defense Security Service personnel were not aware that CPI resided within the prime contractor's and subcontractors' facilities because CPI was not identified in the DD Form 254 provided to cleared contractors. The Defense Security Service should be provided a copy of the program protection plan and the program office's specific requirements for the cleared contractor and the related documents for the protection of CPI and the DD Form 254 should reflect the information needed to protect CPI.

Recommendations, Management Comments, and Our Response

B2-1. We recommend that the Under Secretary of Defense for Acquisition, Technology, and Logistics provide guidance on model contract language in support of program protection planning to DoD and Component RTP officials.

Management Comments

The Under Secretary of Defense for Acquisition, Technology, and Logistics concurred with the recommendation.

Our Response

The comments of the Under Secretary of Defense for Acquisition, Technology, and Logistics are partially responsive in meeting the intent of the recommendation. The Under Secretary of Defense for Acquisition, Technology, and Logistics should provide an action plan and a date for establishing the guidance on model contract language in support of program protection planning.

As a result of management comments, we redirected Recommendation B2-2 from the Director, Defense Security Service to the Deputy Under Secretary of Defense for HUMINT, Counterintelligence, and Security.

B2-2. We recommend that the Deputy Under Secretary of Defense for HUMINT, Counterintelligence, and Security provide guidance on model language in the DD Form 254, in order to provide the Defense Security Service with the information they need to protect critical program information.

Management Comments

The Deputy Under Secretary of Defense for HUMINT, Counterintelligence, and Security concurred with the recommendation to provide guidance on model language in the DD Form 254, in order to provide the Defense Security Service with the information they need to protect critical program information. The Deputy Under Secretary of Defense for HUMINT, Counterintelligence, and Security will revise language in the draft DoD Manual 5200.39-M, to address both classified and unclassified CPI by instructing users to complete the DD Form 254 to ensure that contractors are advised by the Program Manager and that the Defense Security Service is informed of unclassified CPI residing at a contract facility.

Our Response

The comments of the Deputy Under Secretary of Defense for HUMINT, Counterintelligence, and Security are partially responsive in meeting the intent of the recommendation. The Deputy Under Secretary of Defense for HUMINT, Counterintelligence, and Security should provide a date for providing model language in the DD Form 254 through revision of the language in the draft DoD Manual 5200.39-M. If the Deputy Under Secretary of Defense for HUMINT, Counterintelligence, and Security believes that the formal coordination process for the draft manual will prevent timely guidance from reaching program protection officials, then steps should be taken to provide interim guidance, such as a policy letter or directive type memorandum, to ensure timely delivery of changes to the DD Form 254.

Issue Area Three: Training Efforts for the Protection of Critical Program Information

We assessed this issue area to determine whether published guidance for training to identify and protect CPI is relevant to and adhered to by program, intelligence, counterintelligence, and security personnel. We determined that training and education for the protection of CPI was not tailored.

DoD Instruction 5200.39 states that the USD(AT&L) will collaborate with the Under Secretary of Defense (Intelligence) and the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer to require that appropriate training be available to RDA personnel regarding the identification and protection of CPI. Training should include the roles that RDA, sustainment (logistics, maintenance, repair, supply), testing, counterintelligence, intelligence, security, systems engineering, and information systems security engineering personnel perform to identify and protect CPI.

While the amount of experience varied, the majority of the personnel interviewed had many years of experience on major weapon system acquisition programs. However, the level of training related to CPI protection varied. There were personnel with no training, those with training acquired on the job, and others with attendance at training offered by the RDA program support organization.

The level 1 and 2 acquisition courses at the Defense Acquisition University minimally address counterintelligence, intelligence, and security support to RTP. However, to ensure that program personnel have a better understanding of RTP support, the ARTPC offers and conducts acquisition program protection training for its research and technology community. The training entails a review of the program protection process, including the CPI assessment and the generation of the technology protection plan and program protection plan. The Defense Security Service is designing a CPI course for DoD contractors and Government security officers that is scheduled to be ready at the end of 2010.

The Joint Counterintelligence Training Academy offers counterintelligence support to RTP training and provides advanced counterintelligence training to Defense counterintelligence components. The Academy also provides training to other intelligence community personnel on a limited basis. However, the counterintelligence support to RTP training is not structured for non-counterintelligence personnel, who typically provide a large share of the RTP support to PMs.

Conclusion

There was no tailored CPI protection training. Intelligence and security-related training for the protection of CPI is uneven. Training tailored to participants' roles needs to be developed and made available by the organization most able to deliver it effectively and efficiently. Research, development, and acquisition program support organizations, the Defense Acquisition University, and the Defense Security Service should be considered delivery mechanisms for training.

Recommendations, Management Comments, and Our Response

B3. We recommend that the Under Secretary of Defense for Acquisition, Technology, and Logistics, in collaboration with the Under Secretary of Defense for Intelligence, and the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer develop standardized guidance for training in CPI protection for use by the RTP community.

Management Comments

The Under Secretary of Defense for Acquisition, Technology, and Logistics partially concurred, while the Under Secretary of Defense for Intelligence, and the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer concurred with the recommendation to develop standardized guidance for training in CPI protection for use by the RTP community. The Under Secretary of Defense for Acquisition, Technology, and Logistics agreed to develop standardized guidance and training, inclusive of a broader scope of protection for the program protection community, not only the RTP community, stating that RTP does not include the new requirements to protect elements or components critical to network or mission effectiveness in DoD Instruction 5200.39.

Our Response

The comments of the Under Secretary of Defense for Acquisition, Technology, and Logistics, the Under Secretary of Defense for Intelligence, and the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer are partially responsive in meeting the intent of the recommendation. The Under Secretary of Defense for Acquisition, Technology, and Logistics should provide a date for developing standardized guidance for training in CPI protection for use by the program protection community.

Issue Area Four: Use of Resources for the Protection of Critical Program Information

We assessed this issue area to determine whether program, intelligence, counterintelligence, and security personnel assigned to protect CPI are appropriately used.

OASA ALT - (b)(4)

[redacted]

For the WIN-T program, it appeared that the Deputy Chief of Staff, G-2, provided adequate support through the 902nd Military Intelligence Group, the Army Counterintelligence Center, the National Ground Intelligence Center, and the ARTPC.

OASA ALT - (b)(5)

[redacted]

OASA ALT - (b)(4), (b)(5)

[redacted]

Conclusion

WIN-T did not track or report program protection or security-related expenditures. Tracking and reporting these expenditures assist program management offices with budget projections for security throughout the program and with measuring the return on the security expenditures.

OASA ALT - (b)(5)

[redacted]

Because of the many organizations we visited as part of this broad assessment and the level of depth needed to fully assess this issue area; and because we are conducting an assessment to determine how the Department tracks security costs, we make no recommendations for this issue area.

Issue Area Five: Effectiveness of Policies to Protect Critical Program Information

We assessed this issue area to determine whether published guidance for the identification and protection of CPI is relevant to and adhered to by program, intelligence, counterintelligence, and security personnel. We primarily assessed RTP efforts using DoD Instruction 5200.39; however, many issuances, covering many subject areas, and coming from many agencies, that address RTP. There are 145 policies that an acquisition program may need to comply with the vast amounts of policy related to program protection. A hyperlinked-HTML version of a chart, developed by the Office of Systems Analysis, in the Systems Engineering Directorate, overseen by the Director of Defense Research and Engineering, in the office of the USD(AT&L), depicting the policies can be found at http://www.acq.osd.mil/sse/docs/acq-security-policy-tool/index.html.

Because the number of policies is so vast, they require a more in-depth analysis than this limited scope program protection assessment pilot offered. As explained in Finding A, the Army Audit Agency found that the Army did not have a regulation governing RTP. The Army is developing guidance on RTP. It has established a working group that would implement the guidance contained in DoD Instruction 5200.39 on RTP, as well as implement the recommendations in the Army Audit Agency audit related to protecting CPI.

OASA ALT - (b)(4)

[redacted] Guidance on this subject that is referenced in DoD Instruction 5200.39 has yet to be promulgated. Enclosure 2, paragraph 4.b, tasks the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer to "identify minimum security requirements for contractor owned and operated information systems for the protection of CPI." Directive-Type Memorandum 08-027, "Security of Unclassified DoD Information on Non-DoD Information Systems," July 31, 2009, addresses security requirements for contractors processing DoD information on non-DoD information systems and may provide a model for this, but it does not address the protection of CPI specifically. The appropriate guidance can be developed and incorporated in the upcoming CPI protection manual or other RTP-related issuances.

Conclusion

Since December 2008, the Army has ongoing efforts to develop guidance on RTP. It has established a working group to implement the guidance contained in DoD Instruction 5200.39 on RTP, as well as implement the recommendations in the Army Audit Agency's April 29, 2009 report "Army Research and Technology Protection Program: Office of the Assistant Secretary of the Army (Acquisition, Logistics, and Technology)." Guidance has not been developed that specifically addresses the protection requirements for CPI on contractor-owned and -operated information systems.

Recommendations, Management Comments, and Our Response

B5-1. We recommend that the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer, in coordination with the Under Secretary of Defense for Acquisition, Technology, and Logistics, and the Under Secretary of Defense for Intelligence, develop and publish security requirements for contractors processing CPI on contractor-owned and -controlled information systems.

Management Comments

The Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer, the Under Secretary of Defense for Acquisition, Technology, and Logistics, and the Under Secretary of Defense for Intelligence concurred with the recommendation to develop and publish security requirements for contractors processing CPI on contractor-owned and -controlled information systems through a combination of the issuance of Directive Type Memorandum 08-027, DoD Instruction 5205.13, "Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities," January 29, 2010, Under Secretary of Defense for Acquisition, Technology, and Logistics memorandum, "Cyber Security in Defense Acquisition Programs," November 18, 2008, and DoD Federal Acquisition Regulation Supplement Case 2008-D028, "Safeguarding Unclassified Information," which will provide the specific guidance to contracting officers and associated clauses to implement the Directive Type Memorandum in contracts.

Our Response

The comments to the recommendation are partially responsive in meeting the intent of the recommendation. The Under Secretary of Defense for Acquisition, Technology, and Logistics should provide a date for the completion of DoD Federal Acquisition Regulation Supplement Case 2008-D028, "Safeguarding Unclassified Information."

Issue Area Six: Ability of Counterintelligence, Intelligence, and Security to Support the Protection of Critical Program Information

We assessed this issue area to determine whether published guidance to enable counterintelligence, intelligence, and security personnel and programs to support the protection of CPI is relevant to and adhered to by program, intelligence, counterintelligence, and security personnel. We determined that counterintelligence and security were known to WIN-T program staff and did provide required counterintelligence and intelligence support and threat-related data. However, a Technology Targeting Risk Assessment had not been requested. WIN-T program staff were not aware of Defense Security Service personnel, and Defense Security Service was not aware of the existence of WIN-T CPI, nor was the existence of CPI or a program point of contact for reporting violations annotated on the DD Form 254.

DoD Instruction 5200.39 states that the Under Secretary of Defense (Intelligence) will issue policy guidance that requires the heads of DoD Components; with counterintelligence elements and organizations to develop and implement tailored counterintelligence support plans at all DoD research and development facilities, for all RDA programs with CPI, and at facilities of cleared Defense contractors with CPI: to issue policy guidance that requires the heads of DoD Components with intelligence and counterintelligence analytical centers to provide assessments regarding foreign intelligence requirements for and targeting of CPI; DoD Component intelligence analytical centers, in cooperation with the Defense Intelligence Agency, to provide Technology Targeting Risk Assessments[15] to assist RDA programs with mitigating the risk of CPI compromise and to support counterintelligence organizations with developing counterintelligence assessments of CPI; and directs counterintelligence analytical centers to provide counterintelligence assessments for RDA programs with CPI.

Counterintelligence support personnel were known to WIN-T program management office personnel, participated in the CPI identification process, and prepared a counterintelligence support plan. The counterintelligence support plan contained sufficient detail for WIN-T program management office personnel to understand the support that they could expect to receive from counterintelligence support personnel.

Security personnel from CECOM Life Cycle Management Command, G-2, although not embedded in the WIN-T program management office, were known to program staff and had submitted requirements for threat data, with the exception of the Technology Targeting Risk Assessment. The CECOM Life Cycle Management Command, G-2, had also promulgated the System Threat Analysis Report.

---

[15] Country-by-country assessments conducted by the Defense intelligence community that quantify risks to critical program information and related enabling technologies for weapons systems, advanced technologies or programs, and facilities such as laboratories, factories, research and development sites (test ranges, etc.), and military installations. The Technology Targeting Risk Assessment evaluates five independent risk factors, each of which contributes to an overall risk factor. The five areas evaluated are: technology competence, national level of interest, risk of technology diversion, ability to assimilate, and technology protection risk. The Technology Targeting Risk Assessment and counterintelligence assessment provide laboratory/technical directors and PMs with information required to establish a comprehensive security program for the protection of identified critical program information.

In accordance with DoD Instruction 5200.39, the Defense Security Service shall assist DoD Component counterintelligence elements in coordinating the execution of counterintelligence support plans at the facilities of cleared defense contractors with classified CPI. The contract's DD Form 254 should indicate the existence of CPI so that the Defense Security Service will know what areas need enhanced levels of protection. The DD Form 254 also needs to identify cleared defense contractors performing on and employees' access to the locations where classified CPI or unclassified CPI relating to classified contracts reside. The Defense Security Service is developing procedures to centralize the receipt, analysis, and dissemination of such information in a manner that permits maximum control and use. Defense PMs must provide the Defense Security Service a copy of the program protection plan and counterintelligence support plan to adequately provide overlapping counterintelligence support to protect CPI. Identification of all subcontractors performing on specific programs with classified CPI or unclassified CPI on classified programs would improve the protection of CPI.

The Defense Security Service was not informed of the existence of WIN-T CPI. It was not contained in the DD Form 254, and there was no communication between the Defense Security Service and WIN-T program office staff. There should be better communication between the Defense Security Service and the prime contractor. Moreover, there is no place on the DD Form 254 to state which subcontractors possess critical program information. If a program's DD Form 254 specified the existence of unclassified critical program information and the protection measures required, the Defense Security Service could include critical program information protection in its facility inspections. The DD Form 254 should also include a program point of contact for reporting security violations and counterintelligence concerns. While the WIN-T CPI is unclassified, DSS during the conduct of regularly scheduled security inspections at cleared Defense contractor facilities determines if there are any contractually imposed protection measures for CPI related to classified contracts at those locations.

Conclusion

Supporting counterintelligence and security personnel were known to WIN-T program management office personnel. However, the Defense Security Service was not informed of the existence of CPI, and the existence of CPI was also not written into the DD Form 254. It is unclear how lower-tier subcontractors accomplish program protection and, further, how verification of contractor compliance with DD Form 254 below the prime contractor level is accomplished. The DD Form 254 should include a program point of contact for reporting security violations and counterintelligence concerns. While the WIN-T CPI is unclassified, DSS during the conduct of regularly scheduled security inspections at cleared Defense contractor facilities determines if there are any contractually imposed protection measures for CPI related to classified contracts at those locations.

Recommendations, Management Comments, and Our Response

As a result of management comments, we redirected Recommendation B6 from the Director, Defense Security Service to the Deputy Under Secretary of Defense for HUMINT, Counterintelligence, and Security.

B6. We recommend that the Deputy Under Secretary of Defense for HUMINT, Counterintelligence, and Security prepare written guidance to determine:

a. what can and should be contained in the DD Form 254 for the protection of controlled unclassified CPI; and

b. how program protection should be implemented at the level of subcontractors, and how to verify contractor compliance with the DD Form 254 and the program protection plan.

Management Comments

The Deputy Under Secretary of Defense for HUMINT, Counterintelligence, and Security concurred with the recommendation. The Deputy Under Secretary of Defense for HUMINT, Counterintelligence, and Security will add CPI as a separate line item to be considered when completing the form, add instructions for Program Managers to include special CPI instructions, require the prime contractor to maintain and provide authorized government officials with updated lists of all subcontractors participating in their contract/program and indicate which requires access to classified CPI (and/or require access to the CPI at other locations) in conjunction with the performance of their subcontracts, identify central locations at the Defense Security Service for the Program Office to provide program protection plan information to the applicable field offices for prime and subcontractors; indicate whether contractors needs to implement specific technology protection measures at their facilities. The Deputy Under Secretary of Defense for HUMINT, Counterintelligence, and Security will also include this guidance within Enclosure 2, "Responsibilities," and Enclosure 6, "Contract Requirements," of the draft DoD Manual 5200.39-M.

Our Response

The comments of the Deputy Under Secretary of Defense for HUMINT, Counterintelligence, and Security are partially responsive in meeting the intent of the recommendation. The Deputy Under Secretary of Defense for HUMINT, Counterintelligence, and Security should provide a date for implementing the changes to the DD Form 254 described in response to our recommendation. If the Deputy Under Secretary of Defense for HUMINT, Counterintelligence, and Security believes that the formal coordination process for the draft manual will prevent timely guidance from reaching program protection officials, then steps should be taken to provide interim guidance, such as a policy letter or directive type memorandum, to ensure timely changes to the DD Form 254.

Issue Area Seven: Effectiveness of the Foreign Visit Program

We assessed this issue area to determine whether published guidance for foreign visits is relevant to and adhered to by program, intelligence, counterintelligence, and security personnel. We assessed this issue area because in a policy letter, "Accountability of Department of Defense (DoD) Sponsored Foreign Personnel in the United States (U.S.)," May 18, 2004, the Deputy Secretary of Defense requires all Inspectors General to verify compliance with the sponsored foreign personnel policy through their inspection processes. We also assessed this issue area to ensure that decisions to grant foreign nationals access to classified and controlled unclassified information during their visits to DoD Component and cleared contractor facilities are consistent with the security and foreign policy interests of the United States and DoD Directives 5230.11, 5230.20, and 5530.3.[16] If there is to be foreign involvement in any aspect of a program or foreign access to the system or its related information, the program protection plan should contain provisions to deny inadvertent or unauthorized access.

The WIN-T program management office currently does not have any foreign government or international organization involvement in program development. OASA ALT - (b)(5)

OASA ALT - (b)(5)

[redacted]

Conclusion

Because the WIN-T program management office does not have involvement by any foreign government or international organization in a cooperative development arrangement at this time, we make no recommendations for this issue area.

[16] DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992; DoD Directive 5230.20, "Visits and Assignments of Foreign Nationals," June 22, 2005; and DoD Directive 5530.3, "International Agreements," June 11, 1987.

Issue Area Eight: Application of Horizontal Protection of Critical Program Information

We assessed this issue area to determine whether published guidance for horizontal protection is relevant to and adhered to by program, security, intelligence, and counterintelligence personnel. We assessed this issue area to ensure that critical Defense technologies, to include CPI, associated with more than one RDA program are protected to the same degree by all involved DoD activities. DoD Instruction 5200.39 states that it is DoD policy to conduct comparative analysis of defense systems technologies and align CPI protection activities horizontally throughout DoD. It also states that the Under Secretary of Defense (Intelligence), in coordination with the USD(AT&L) and the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer, will require the establishment of a database for RDA organizations to record and track CPI for horizontal protection, compromise, and analysis purposes.

The Acquisition Security Database, a horizontal protection database originally created by the U.S. Navy, can provide the RTP community with greater access to CPI. However, the Acquisition Security Database is not used by all Defense RDA components. The Air Force had developed its own horizontal protection database. Use of a horizontal protection database by the RDA community would represent an important step toward the protection of DoD's CPI. Once the RDA community is populating a horizontal protection database, RTP practitioners will be able to view all programs with similar CPI to help ensure consistent RTP support.

OASA ALT - (b)(5)

[redacted]

The DoD Instruction 5200.39 requirement that a horizontal protection database be used in support of the identification of CPI appears to be effective for the WIN-T program.

OASA ALT - (b)(5)

[redacted]

Conclusion

OASA ALT - (b)(5) [redacted]

OASA ALT - (b)(5) [redacted] The DoD Instruction 5200.39 requirement that a horizontal protection database should be used in support of the identification of CPI appears to be effective for the WIN-T program.

OASA ALT - (b)(5) [redacted]

Recommendations, Management Comments, and Our Response

As a result of management comments, we redirected the lead for Recommendation B8 from the Under Secretary of Defense for Intelligence to the Under Secretary of Defense for Acquisition, Technology, and Logistics.

B8. We recommend that the Under Secretary of Defense for Acquisition, Technology, and Logistics, in coordination with the Under Secretary of Defense for Intelligence and the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer, determine the appropriateness of using OASA ALT (b)(5) [redacted]

Management Comments

The Under Secretary of Defense for Acquisition, Technology, and Logistics, the Under Secretary of Defense for Intelligence, and the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer concurred with the recommendation to determine the appropriateness of using OASA ALT (b)(5) [redacted] however, the Under Secretary of Defense for Intelligence non-concurred with the lead being under their cognizance, but instead stated the recommendation should be under the cognizance of the Under Secretary of Defense for Acquisition, Technology, and Logistics as the data owner. The Under Secretary of Defense for Acquisition, Technology, and Logistics agreed. In compliance with DoD Instruction 5200.39, the Under Secretary of Defense for Acquisition, Technology, and Logistics through a memorandum of understanding with the Navy OASA ALT - (b)(5) [redacted]

Our Response

The comments are responsive and meet the intent of the recommendation.

Appendix A. Scope and Methodology

This assessment was conducted in accordance with Quality Standards for Inspections.[17] Those standards require that we plan and perform the assessment to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our assessment objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our assessment objectives. We conducted site visits and a majority of the interviews for this assessment from March 2009 through September 2009, with additional clarifying interviews extending to the publication of this draft report.

The overall assessment scope was broad, encompassing DoD counterintelligence, intelligence, security, and program personnel to protect CPI. We did not assess research, sustainment, or demilitarization phases, nor did we include special access programs in the scope of this assessment. Our scope did not include Section 254 of the FY 2009 National Defense Authorization Act, "Trusted Defense Systems." Section 254 requires the Office of the Secretary of Defense to conduct assessments of selected acquisition programs to identify vulnerabilities in the supply chain of each program's electronics and information processing systems that potentially compromise the level of trust in the systems. The Offices of the USD(AT&L) and the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer led a detailed effort, in conjunction with other DoD elements, to conduct the vulnerability assessments and reported to Congress as required.

For our methodology, we issued an overarching announcement letter to the Department on June 18, 2008, "Assessment of DoD Efforts to Protect Critical Program Information" (Project No. D2008-DINT01-0242.000), which encompassed the eight key issue areas. The eight issue areas related to CPI identification and program protection planning evolved from a series of inspections conducted by the Service Inspectors General and an overarching integrated process team chartered by the Deputy Secretary of Defense in 2000. The overarching integrated process team identified 27 tasks that would enhance the Department's ability to identify and protect CPI, the effectiveness of the foreign visitor program, and the effectiveness of counterintelligence and security support to RDT&E facilities and the acquisition process. We categorized these 27 tasks into the eight key issue areas that are the objectives of this pilot and the subsequent assessments. Within the framework of these eight issue areas, we specifically focused on and assessed standardization of protection processes and their application, oversight of the protection process and its implementation, and responsibility for protection. The eight issue areas are the cornerstone issues of RTP and will be the focus of our future oversight efforts.

On December 12, 2008, we forwarded a letter co-signed by the DoD Office of Inspector General, Deputy Inspector General for Intelligence and the Deputy Under Secretary of Defense (Acquisition and Technology) to the Service Acquisition Executives informing them of the program protection pilot and the need to assess how well the Department identifies and protects CPI and the attendant program protection planning process.

[17] The standards were published by the President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency, which the Inspector General Reform Act of 2008 combined in creating the Council of the Inspectors General on Integrity and Efficiency.

In conjunction with the Office of the Deputy Under Secretary of Defense (Acquisition and Technology), we selected a statistical sample of 17 ACAT ID programs of record from the major defense acquisition program list to participate in an initial questionnaire phase for this program protection pilot assessment. In a subsequent phase, we selected three programs of record, one from each Service, for in-depth assessment.

To ensure that the DoD Office of Inspector General enhances its ability to provide oversight of component Inspectors General audits, evaluations, inspections, and law enforcement activities - and because it was essential to gain a solid understanding of how effectively the Department protects CPI in order to maintain our technological advantage and deliver uncompromised weapon systems to the warfighter--we planned and performed this assessment in coordination with subject matter experts from the Offices of the Under Secretaries of Defense for Acquisition, Technology, and Logistics, for Policy, and for Intelligence; the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer, and the Defense Security Service. Although the subject matter experts contributed to this project, the project results and recommendations are those of the DoD Office of Inspector General.

We wanted to assess a program of record that was in the early stage, one that was almost at the conclusion, and one that had completed program protection planning. This methodology would provide us with an evolutionary perspective of program protection planning. OASA ALT - (b)(5)

[redacted]

Use of Computer-Processed Data
We did not use computer-processed data to perform this assessment.

Appendix B. Prior Coverage

During the last 10 years, the Government Accountability Office (GAO) and the Department of Defense Inspector General (DoD IG) have issued 11 reports discussing DoD and Army efforts to protect critical program information. Unrestricted GAO reports can be accessed over the Internet at http://www.gao.gov. Unrestricted DoD IG reports can be accessed at http://www.dodig.mil/Ir/reports.

GAO

GAO Report No. GAO-09-271, "GAO High-Risk Series – An Update," January 2009

GAO Report No. GAO-08-467SP, "Assessments of Selected Weapons Programs," March 2008

GAO Report No. GAO-08-91, "Departmentwide Direction is Needed for Implementation of the Anti-tamper Policy," January 2008

GAO Report No. GAO-04-302, "DoD Needs to Better Support Program Managers' Implementation of Anti-Tamper Protection," March 2004

DoD IG

DoD IG Report No. 08-INTEL-09, "Report on FY 2007 Summary Report of Inspections on Security, Technology Protection, and Counterintelligence Practices at DoD Research, Development, Test and Evaluation Facilities," June 23, 2008

DoD IG Report No. 08-INTEL-04, "Inspection Guidelines for DoD Research and Technology Protection, Security and Counterintelligence for 2008," April 18, 2008

DoD IG Report No. 07-INTEL-11, "FY 2006 Summary Report of Inspections on Security, Technology Protection, and Counterintelligence Practices at DoD Research, Development, Test and Evaluation Facilities," August 31, 2007

DoD IG Report No. 06-INTEL-14, "FY 2005 Summary Report of Inspections on Security, Technology Protection, and Counterintelligence Practices at DoD Research, Development, Test and Evaluation Facilities," September 20, 2006

DoD IG Report No. 06-INTEL-03, "Inspection Guidelines for DoD Research and Technology Protection, Security and Counterintelligence for 2006," February 28, 2006

DoD IG Report No. 05-INTEL-14, "FY 2004 Summary Report of Inspections on Security, Technology Protection, and Counterintelligence Practices at DoD Research, Development, Test and Evaluation Facilities," May 27, 2005

DoD IG Report No. 00-OIR-05, "Measures to Protect Against the Illicit Transfer of Sensitive Technology," March 27, 2000

Appendix C. Additional Background Information

Historical Perspective. In early 1999, the Deputy Secretary of Defense directed the Service Inspectors General to survey the counterintelligence and security programs at more than 60 RDT&E facilities. The teams identified a number of recommendations related to the specific sites. As a result of these efforts, the Deputy Secretary of Defense chartered an Overarching Integrated Process Team to better frame the recommendations and to oversee their implementation. From February 12 to May 12, 2000, the Deputy Secretary of Defense signed a total of 7 memoranda containing 27 tasks aimed at enhancing the Department's ability to identify and protect CPI, implement an effective foreign visitor program, and provide effective counterintelligence and security support to RDT&E facilities and the acquisition process. On February 17, 2000, the Deputy Secretary of Defense signed a memorandum requesting the DoD Inspector General to ensure that DoD Components implement a uniform system of periodic reviews through their existing agency and Service inspection processes for compliance with directives concerning security, technology protection, and counterintelligence practices. These reviews were to assist with the protection of the cutting edge technology of U.S. weapon systems. The February 17, 2000 memorandum also requested that the DoD Inspector General develop inspection list guidelines for all Department Inspectors General to enhance consistency. The Deputy Secretary of Defense's requests to the DoD Inspector General are also outlined in DoD Instruction 5200.39.

On May 8, 2002, the Inspector General, DoD; the Deputy Under Secretary of Defense for Laboratories and Basic Sciences; the Director, Operational Test and Evaluation; the Service Inspectors General; and the Director, Program Integration, Internal Management Review (formerly Internal Assessments), Missile Defense Agency, signed a memorandum of understanding on security, technology protection, and counterintelligence inspections. The memorandum of understanding requires participating Inspectors General to prepare and forward to the DoD Office of Inspector General any significant findings and recommendations at the end of each inspection. The DoD Office of Inspector General[18] issues a summary report on inspections of security, technology protection, and counterintelligence practices at DoD RDT&E facilities.

[18] Since the original request by the Deputy Secretary of Defense, the Office of the Deputy Inspector General for Intelligence, in the DoD Office of Inspector General, has published the annual summary report, highlighting Service and milestone decision authority inspections and best practices. We also publish the guidelines biennially, with input from Department and Component counterintelligence, intelligence, security, and Inspectors General elements.

Appendix D. DoD Organizations and Efforts to Protect Critical Program Information

Establishing a consistent process for identifying CPI and conducting program protection planning, a process that takes into account the role research, development, acquisition, counterintelligence, intelligence, security, and systems engineering personnel perform, is critical for ensuring that DoD can protect CPI. In December 2008, DoD established nine working groups to address CPI identification and program protection planning. The working group process is co-led by the offices of the USD(AT&L) and the Under Secretary of Defense (Intelligence). Each working group is chaired by either a DoD or Service representative with expertise in the protection of CPI. DoD has agreed that there should be an overarching set of program protection products (for example, process, guidance, tools) and that these would be extended and amplified by the Services and agencies to serve their needs. One of the goals of these working groups is for the Services and agencies to assess the sufficiency of resources available to support program protection when the program protection processes are sufficiently mature to form a basis for such an assessment.

Program Protection Working Groups

Definitions Working Group. This working group will expediently affirm and document the CPI, program protection, systems assurance, and software assurance terms and associated hierarchy of relationships. Completion of this working group was described as being necessary to initiate the other working groups.

CPI Identification Process Working Group. This working group is to establish the minimum standards for the process used by DoD to identify CPI. Services and agencies will be allowed to extend and amplify to suit their Service or agency needs. A second product will be a method of assessing the tools used by various Services and agencies to identify CPI. The working group will use, as appropriate, the results from other groups.

Program Protection Planning Content, Format, and Review Working Group. This working group will develop two products. The first product will be guidance on preparing program protection plans. The second product will document the program protection plan review process and stakeholders. The program protection plan review process will detail milestone requirements (with checklists) for development, review, and approval; stakeholders include Service components, the USD(AT&L), the Under Secretary of Defense (Intelligence), and subject matter experts for applicable countermeasures such as anti-tamper measures, and Defense trusted integrated circuits. The first draft of the program protection plan review process was based on the systems engineering plan[19] process and will be revised in a Six Sigma working group.

---

[19] The systems engineering plan is the blueprint for the execution, management, and control of the technical aspects of an acquisition program from conception to disposal. Systems engineering translates operational requirements into configured systems, integrates technical inputs of the entire design team, manages interfaces, characterizes and manages technical risk, transitions technology from the technology base into program specific efforts, and verifies that designs meet operational needs. The systems engineering plan is a "living" document that captures a program's current and evolving systems engineering strategy and its relationship with the overall program management effort.

Acquisition Policy and Guidance for Program Protection Working Group. This working group will aid in the development of program protection guidance to be documented in the upcoming DoD 5200.39 Manual. The working group will build on all other working group outputs and ensure consistency with the DoD Instruction 5000.02.

Training and Transition Working Group. This group will develop a competency model for program protection roles. Based on the preliminary work done by the Program Protection Working Group, this working group will confirm the required skills, define the course content to serve the needs of the various functional areas (acquisition, engineering, counterintelligence, criminal investigative service, and the like), and estimate the number of courses required per year to accommodate the training of the workforce. This working group will also develop and implement a plan to train service personnel and transition to the revised program protection process and policy.

Horizontal Protection Process Working Group. This working group will define process flow, roles, responsibilities, and policy to execute horizontal protection from before milestone A through sustainment. The first task will be to determine the need for a standardized security classification guide for program protection. The work of this team will be submitted to the Under Secretary of Defense (Intelligence) for consideration in the development of the next version of DoD 5200.1-R, "Information Security Program," the current version of which is dated January 1997. This group will also work to provide input to the Acquisition Security Database Configuration Control Board and to incorporate the Acquisition Security Database within Service policy and processes.

Manpower Studies Working Group. Formation of this working group will depend on each Service making a determination whether or not to act on the proposal of the Program Protection Working Group to conduct manpower studies to assess the sufficiency and availability of resources to support the program protection process.

Criticality Assessment Working Group. This working group will develop the process required to implement system security engineering in program protection planning. Membership will include primarily systems engineers and individuals familiar with program risk mitigation as currently implemented by programs.

Vulnerability Process Working Group. This working group will define the process and criteria for the vulnerability assessment step in the program protection process. The scope of the vulnerabilities assessment will include the acquisition development and manufacturing environments, supply chain, operational environment, and system design.

Under Secretary of Defense for Intelligence

The Under Secretary of Defense for Intelligence began promulgating policy for counterintelligence support in 2009 to the RDA community. The policy will implement the relevant sections of policy established in DoD Instruction 5200.39 for counterintelligence support to the protection of CPI; DoD Instruction 2040.02, "International Transfers of Technology, Articles, and Services," July 10, 2008, for counterintelligence support to international transfers of technology, articles, and services; and Deputy Secretary of Defense Directive-Type Memorandum 08-048, "Supply Chain Risk Management(SCRM) to Improve the Integrity of Components Used in DoD Systems," February 19, 2009, for counterintelligence support to supply-chain risk management.

The new policy will establish a requirement for an intelligence assessment of DoD RDA programs to provide baseline security requirements against foreign intelligence collection. It will also integrate a technology threat risk assessment with the appropriate counterintelligence analytical product to inform RDA programs of threats to CPI from foreign intelligence entities. It is currently in the formal coordination process.

The Under Secretary of Defense (Intelligence) is also in the process of finalizing DoD Manual 5200.39, "Procedures for Critical Program Information (CPI) Protection Within the Department of Defense," which will provide the guidance for the implementation of program protection measures. It is currently in the formal coordination process.

Defense Intelligence Agency

The Defense Intelligence Agency provides risk assessment products on foreign threats [redacted] coordinates with DoD Component counterintelligence elements on horizontal protection in support of the protection of CPI. The Defense Intelligence Agency produces the Technology Targeting Risk Assessments and [redacted]

DIA - (b)(3): 10 U.S.C. § 424

DIA - (b)(3): 10 U.S.C. § 424

Defense Security Service

U.S. industry develops and produces the majority of our Nation's defense technology, much of which is classified, and thus plays a significant role in creating and protecting the information that is vital to our Nation's security. The National Industrial Security Program was established by Executive Order 12829 to ensure that cleared U.S. facilities safeguard the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. The Defense Security Service administers the National Industrial Security Program on behalf of DoD and 23 other Federal agencies. Defense Security Service has responsibility for over 13,000 active, cleared facilities in the National Industrial Security Program.

The Defense Security Service supports national security and the warfighter, secures the Nation's technological base, and oversees the protection of U.S. and foreign classified information in the hands of industry. The Defense Security Service accomplishes this mission by performing six mission-essential tasks:

- clearing industrial facilities, personnel, and accrediting associated information systems;
- counterintelligence support to cleared industry and referral of counterintelligence relevant information to applicable counterintelligence community members and law enforcement agencies;
- managing foreign ownership, control, and influence in cleared industrial facilities;
- providing advice and oversight to industry;
- delivering security education and training; and
- conducting mission support operations.

To accomplish this mission, the Defense Security Service has approximately 270 industrial security representatives and approximately 50 field counterintelligence specialists spread across the United States. They provide oversight and assistance to cleared contractor facilities and assist the organization's management and facility security officers in ensuring the protection of national security information.
The Defense Industrial Security Clearance Office processes requests for industrial personnel security investigations and provides eligibility or clearance determinations for cleared industry personnel under the National Industrial Security Program.

The Defense Security Service Academy delivers security education and training to DoD civilians, military, and other U.S. Government personnel, National Industrial Security Program contractors, and sponsored representatives of foreign governments.

The Defense Security Service Counterintelligence Directorate provides counterintelligence functional services in support of DoD RDA, as described below.

- Defense Security Service identifies unlawful penetrations to facilities cleared in conjunction with the National Industrial Security Program.

- Defense Security Service counterintelligence prepares and provides relevant threat information, awareness briefings, and tailored analytical products to cleared defense contractors as determined necessary based on prioritized risk levels and specific requests from cleared defense contractors.

- The Defense Security Service counterintelligence office produces an annual report, "Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry." The Defense Security Service encourages cleared defense contractors to use this information for security awareness and education programs at their facilities.

Appendix E. Army Organizations and Efforts to Protect Critical Program Information

902nd Military Intelligence Group

The 902nd Military Intelligence Group's technology protection mission is to detect, identify, neutralize, and exploit foreign intelligence service threats to Army technologies. The Group identifies investigative and operational opportunities within the acquisition and RDT&E communities while providing for the secure fielding of Army technologies, capabilities, and weapon systems. The 902nd Military Intelligence Group employs counterintelligence covering agent support to acquisition PMs and Army research facilities to ensure detailed familiarity with the supported element's operations, personnel, security, and vulnerabilities. In turn, the Group provides the element with a point of contact for reporting matters of counterintelligence interest. The Group augments covering agents with technical, analytical, investigative, and operational resources to neutralize or exploit foreign intelligence threats.

Army Counterintelligence Center

The Army Counterintelligence Center is the Army's counterintelligence analysis and production center. The Army Counterintelligence Center's mission is to provide timely, accurate, and effective multidisciplinary counterintelligence analysis in support of the U.S. Army combating terrorism program, ground system technologies, and counterintelligence investigations, operations, and activities. The Army Counterintelligence Center provides the multidisciplinary counterintelligence threat assessment to Army program offices to assist with the evaluation of risk, based on threats to the program's CPI. The Center supports Army, DoD, and non-DoD customers.

National Ground Intelligence Center

The mission of the National Ground Intelligence Center is to provide science and technical intelligence and general military intelligence on foreign ground forces. The Center supports the warfighting commanders; force and material developers; and Department of the Army, DoD, and national decision makers. [redacted] INSCOM - (b)(7)(E)

Army Defense Industrial Base Cyber Security Office

The Army Defense Industrial Base Cyber Security Office works across the Army to integrate the requirements to protect CPI identified in DoD Instruction 5200.39 through interface with Army program executive offices and their respective program/product managers and with the Army Materiel Command to ensure synchronization of Army priorities and requirements established for RTP and critical infrastructure protection programs. Also, when technologies similar to those used by the Army are found in other Military Service research and development programs and weapon systems, the Army Defense Industrial Base Cyber Security Office coordinates with the USD(AT&L) and the other Service acquisition authorities to ensure like technologies are afforded the same level of protection.

The Army Defense Industrial Base Cyber Security Office is leading Components of the Office of the Secretary of Defense in a tri-Service cyber security acquisition initiative that is intended to provide DoD with an empirical basis -including viable contract language, budgetary ramifications and Defense Federal Acquisition Regulation Supplement/Federal Acquisition Regulation revisions-to evaluate potential solutions for protecting controlled unclassified information on defense industrial base networks.

The Army Defense Industrial Base Cyber Security Office is coordinating an interagency pilot program to assess information compromised through computer intrusions against defense industrial base contractor systems to determine whether there may have been compromises of data on current and future Army weapons programs, scientific and research projects, and warfighting capabilities that could cause a loss of technological advantage against potential adversaries.

The Army Defense Industrial Base Cyber Security Office is working with elements of the Office of the Secretary of Defense, including the USD(AT&L), the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer, and others, to develop policy to manage the risk that adversaries might insert corrupted or malicious technology into components – some of which may come from outside the U.S. defense industrial base – that are bound for DoD critical systems to later gain unauthorized access to data, alter data, or sabotage communications. The focus of the Army effort will be on companies in the command, control, communications, intelligence, surveillance, and reconnaissance categories, and on technologies that affect Army modernization efforts or the security of RDT&E facilities, program offices, or supply chains.

The Army Defense Industrial Base Cyber Security Office has developed cooperative relationships across the Army and DoD. To standardize RDA activities and to ensure it incorporates best practices from across the Army, the Defense Industrial Base Cyber Security Office has taken the lead within an Army working group to draft a regulation on protecting CPI.

Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics Comments

OFFICE OF THE DIRECTOR OF
DEFENSE RESEARCH AND ENGINEERING
3040 DEFENSE PENTAGON
WASHINGTON, DC 20301-3040

JUN 11 [illegible]

MEMORANDUM FOR DEPUTY ASSISTANT INSPECTOR GENERAL, INTELLIGENCE EVALUATIONS, DoDIG

THROUGH: DIRECTOR, ACQUISITION RESOURCES AND ANALYSIS 6/14/10

SUBJECT: Response to DoDIG Draft Report on DoD Efforts to Protect Critical Program Information: The Army's Warfighter Information Network – Tactical (Project No. D2008-DINT01-0242.001)

As requested, I am providing responses to the general content and recommendations contained in the subject report.

Recommendation B1-1:
We recommend that the Under Secretary of Defense (Acquisition, Technology, and Logistics), in consultation with the Undersecretary of Defense (Intelligence), the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer, and Component RTP [redacted] OASA ALT - (b)(5)

Response:
Concur. [redacted] OASA ALT - (b)(5)

Anti-Tamper (AT) policy now resides in DoD Instruction 5200.39, "Critical Program Information (CPI) Protection Within the Department of Defense," July 16, 2008, and DoD Instruction 5000.02, "Operation of the Defense Acquisition System," December 8, 2008. In addition, an Anti-Tamper appendix resides within the draft DoD Manual 5200.39-M, "Procedures for Critical Program Information (CPI) Protection within the Department of Defense," which is currently in comment adjudication by the Undersecretary of Defense for Intelligence.

The AT Executive Agent (ATEA) published the second version of its classified SECRET AT Guidelines, which contain a common engineering methodology that guides

Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics Comments

a Program Manager in the establishment of an appropriate AT architecture for the protection of CPI across the entirety of a program's lifecycle. The ATEA also teaches an AT Short Course, which includes content on:

- DoD Anti-Tamper policy directives
- the process of specifying, designing and evaluating AT technology
- anti-tamper design milestones and their relationship to the acquisition cycle
- models of security, including protection, detection, and response approaches
- reverse engineering threats to hardware and software systems
- anti-tamper techniques including encryption and protected volumes

The DoD AT integrated Product Team (IPT), established by USD(AT&L) in 2009, oversees the DoD AT program from a strategic perspective. The IPT consists of representatives from USD(I), NII, and other OSD offices, and has been briefed by Army, Navy, and Air Force anti-tamper representatives on current status and issues.

Recommendation B1-2:
We recommend that the Under Secretary of Defense (Acquisition, Technology, and Logistics) establish guidance for identifying commercial off-the-shelf/government off-the-shelf components as critical program information, to include assessment tools and training.

Response:
Concur. USD(AT&L) is currently working with USD(I), ASD(NII)/DoD CIO, and the Components to establish guidance for the identification of Critical Program Information, to include elements or components critical to network or mission effectiveness per DoD Instruction 5200.39. These elements or components may be commercial off-the-shelf/government off-the-shelf, and the guidance will allow for identification of those components as CPI.

Recommendation B2-1:
We recommend that the Under Secretary of Defense (Acquisition, Technology, and Logistics) provide guidance on model contract language in support of program protection planning to DoD and Component RTP officials.

Response:
Concur. USD(AT&L) will provide guidance on the model contract language in support of program protection planning to DoD and component RTP officials in accordance with DoD Instruction 5200.39 and FAR subpart 15.204.1.

DoD Instruction 5200.39 requires that contracts supporting RDA programs where CPI has been identified shall contain contractual terms requiring the contractor to protect the CPI to the standards articulated in the Instruction. Programs are responsible for

Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics Comments

getting Program Protection requirements written into the contract. Guidance on Program Protection requirement language for CPI Protection is under development.

FAR subpart 15.204.1 specifies the format and content of RFP solicitations and contracts. The RFP includes the terms and conditions that will be in the final contract.

Recommendation B3:
We recommend that the Under Secretary of Defense (Acquisition, Technology, and Logistics), in collaboration with the Undersecretary of Defense (Intelligence), and the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer develop standardized guidance for training in CPI protection for use by the RTP community.

Response:
Partial Concur. USD(AT&L) will, in collaboration with USD(I) and ASD(NII)/DoD CIO, develop standardized guidance for training in CPI protection for use by the *program protection* community, not only the RTP community. Research and Technology Protection remains a critical portion of Program Protection Planning, but does not include the new requirements to protect elements or components critical to network or mission effectiveness per DoD Instruction 5200.39. Training modules will reflect the need to address this broader scope of protection. Training modules will be developed once USD(AT&L), in collaboration with USD(I), ASD(NII)/DoD CIO, and the Components, establishes guidance on CPI identification and protection.

Recommendation B5-1:
We recommend that the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer, in coordination with the Under Secretaries of Defense for Acquisition, Technology, and Logistics and for Intelligence, develop and publish security requirements for contractors processing CPI on contractor owned and controlled information systems.

Response:
Concur. USD(AT&L) will continue to support ongoing efforts by the ASD(NII)/DoD CIO in accordance with DoD Instruction 5205.13, "Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities," January 29, 2010, and USD(AT&L) Memorandum "Cyber Security in Defense Acquisition Programs," November 18, 2008.

Recommendation B8:
We recommend that the Under Secretary of Defense (Intelligence), in coordination with the Under Secretary of Defense (Acquisition, Technology, and Logistics), and the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer, determine the appropriateness of using OASA ALT (b)(5) [redacted]

Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics Comments

Response:
Concur. OASA ALT - (b)(5) [redacted]

OASA ALT - (b)(5) [redacted]

Classification Review:
Concur with the For Official Use Only markings on the subject report.

Please contact DoD OIG - (b)(6) [redacted] @osd.mil, if additional information is required.

Stephen P. Welby
Director
Systems Engineering

Office of the Under Secretary of Defense for Intelligence Comments

OFFICE OF THE UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

INTELLIGENCE

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
(ATTN: DoD OIG - (b)(6))

SUBJECT: Review of Draft Report: DoD Efforts to Protect Critical Program Information: The Army's Warfighter Information Network – Tactical (Project No. D2008-DINT01-0242.001)

In response to your April 9, 2010 memorandum, we provide the attached comments on the subject report. My point of contact is DoD OIG - (b)(6) at DoD OIG - (b)(6) or DoD OIG - (b)(6)@osd.mil.

Stanley L. Sims
Director of Security

Attachment:
As stated

Office of the Under Secretary of Defense for Intelligence Comments

RECOMMENDATION B1-1. *We recommend that the Under Secretary of Defense (Acquisition, Technology, and Logistics), in consultation with the Under Secretary of Defense (Intelligence), the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer, and Component RTP officials,* OASA ALT - (b)(5) [redacted]

RESPONSE: CONCUR. OASA ALT - (b)(5) [redacted]

RECOMMENDATION B3. *We recommend that the Under Secretary of Defense (Acquisition, Technology, and Logistics), in collaboration with the Under Secretary of Defense (Intelligence), and the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer develop standardized guidance for training in CPI protection for use by the RTP community.*

RESPONSE: CONCUR. DoDI 5200.39, "Critical Program Information Protection within the Department of Defense," requires that appropriate training be made available to counterintelligence, intelligence, security, and RDA personnel regarding the identification and protection of CPI. Enclosure 2 of the instruction provides guidelines. DoD standards for CPI identification and protection are under development in the RTP community; as these standards mature, training and specific course content will be developed. Currently, the Joint Counterintelligence Training Academy offers a Counterintelligence Support to RDA course for counterintelligence professionals.

RECOMMENDATION B5-1. *We recommend that the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer, in coordination with the Under Secretaries of Defense for Acquisition, Technology, and Logistics and for Intelligence, develop and publish security requirements for contractors processing CPI on contractor-owned and -controlled information systems.*

RESPONSE: CONCUR. OUSD(I) provided advice and guidance to the OASD(NII)/DoD CIO during the development and promulgation of Directive-Type Memorandum 08-27, "*Security of Unclassified DoD Information on Non-DoD*

Office of the Under Secretary of Defense for Intelligence Comments

Information Systems," and DoDI 5205.13, *"Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities."* These issuances provide guidance for the control of unclassified information, to include CPI that resides on contractor-owned and -controlled information systems. Guidance for the control of classified CPI located on contractor-owned and -controlled information systems is governed by DoD 5220.22-M, *"National Industrial Security Operating Manual."*

RECOMMENDATION B8. *We recommend that the Under Secretary of Defense (Intelligence), in coordination with the Under Secretary of Defense (Acquisition, Technology, and Logistics), and the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer, determine the appropriateness of using* OASA ALT (b)(5) [redacted]
OASA ALT (b)(5)

RESPONSE: NON-CONCUR. OASA ALT - (b)(5) [redacted]

Office of the Deputy Under Secretary of Defense for HUMINT, Counterintelligence, and Security Comments

OFFICE OF THE UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

INTELLIGENCE

JUN 17 2010

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
(ATTN: DoD OIG - (b)(6))

SUBJECT: Defense Security Service (DSS) Response to DoD IG Draft Report: DoD Efforts to Protect Critical Program Information: The Army's Warfighter Information Network – Tactical (Project No. D2008-DINT01-0242.001)," April 2, 2010

In response to your June 3, 2010, request for review of the subject response, we concur and provide the attached comments. My point of contact is DoD OIG - (b)(6) at DoD OIG - (b)(6) or DoD OIG - (b)(6)@osd.mil.

Stanley L. Sims
Director of Security

Attachment:
As stated

Office of the Under Secretary of Defense for Intelligence Comments

RECOMMENDATION B2-2: *We recommend that the Director, Defense Security Service provide guidance on model language in the DD Form 254, in order to provide the Defense Security Service with the information they need to protect Critical Program Information.*

DSS RESPONSE: In accordance with the Office of the Deputy Under Secretary of Defense for HUMINT, CI, and Security (DUSD (HCI&S)) is responsible for policy governing language of the DD Form 254, not the Director, Defense Security Service.

DSS recommends that DUSD(HCI&S) revise language in the draft DoD 5200.39-M to address both classified and unclassified CPI where instructing users to complete the DD Form 254 to ensure the contractors are advised by the program manager and that DSS is formed of unclassified CPI residing at a contract facility.

OUSD(I) RESPONSE: CONCUR. We concur with the response provided by DSS. As the office of primary responsibility for Industrial Security policy, presumably, this office is also responsible for governing language of the DD Form 254, "Contract Security Classification Specification, Department of Defense." The recommended language DSS proposed will be incorporated in Enclosure 2, "*Responsibilities*," of the current draft version of DoD Manual 5200.39-M.

RECOMMENDATION B6: *We recommend that the Director, Defense Security Service, determine and prepare written guidance to:*

a. What can and should be contained in the DD Form 254 for the protection of controlled unclassified CPI; and

OASA ALT - (b)(5)

[redacted]

DSS RESPONSE: As stated in our response in B2-2, the DUSD (HCI&S) and not DSS is responsible for policy changes relating to the DD Form 254.

DSS recommends:

- Block 10, add CPI as a separate line item to be considered when completing the form.

[redacted]

Office of the Deputy Under Secretary of Defense for HUMINT, Counterintelligence, and Security Comments

- Instructions in blocks 13 and 14 should instruct the program manager to include special CPI instructions (i.e. Program Protection Plan (PPP), Classification Guide, etc).

- The prime contractor must maintain and provide authorized government officials with updated lists of all subcontractors participating in their contract/program and indicate which requires access to classified CPI (and/or require access to the CPI at other locations) in conjunction with performance of their subcontracts.

- Identify central locations at DSS for the Program Office to provide PPP information (Review/extraction of applicable information and then expedite distribution to the applicable field offices for prime and subcontractors by ISFO.

- Have space for location of DSS central PPP repository as well as the address of the cognizant DSS Field Office.

- Indicate whether contractor(s) need(s) to be implement specific technology protection measures at their facility(ies).

OUSD(I) RESPONSE: CONCUR. DSS's recommended actions will be appropriately addressed within Enclosure 2, "*Responsibilities*," and Enclosure 6, "*Contract Requirements*," of draft DoD Manual 5200.39-M, "*Procedures for Critical Program Information Protection Within the Department of Defense*."

3

[redacted]

Office of the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

NETWORKS AND INFORMATION INTEGRATION

MEMORANDUM FOR DEPUTY ASSISTANT INSPECTOR GENERAL FOR INTELLIGENCE EVALUATIONS, DoD INSPECTOR GENERAL

SUBJECT: Response to IG Draft Report No D2008-DINT01-0242.001 "DoD Efforts to Protect Critical Program Information: The Army's Warfighter Information Network - Tactical"

This is in response to your memorandum of April 9, 2010 requesting comments pertaining to the subject draft report's recommendations.

With regards to recommendations B1-1, B-3, and B-8, we agree with the recommendations. In these recommendations ASD(NII)/DoD CIO is identified as providing support. For each of these recommendations DASD(IIA) is committed to provide consultation and support as requested by the lead organizations.

With regards to recommendation B5-1, we agree with the recommendation. Our action on this recommendation was completed with the issuance of Directive-Type Memorandum (DTM) 08-027 "Security of Unclassified DoD Information on Non-DoD Information Systems" on 31 July 2009. This issuance addresses the protection of critical program information on contractor systems. The DTM was coordinated with USD(AT&L) and USD(I) through the SD 106 process. In concert with the DTM, USD(AT&L) initiated DoD Federal Acquisition Regulation Supplement (DFARS) Case 2008-D028 "Safeguarding Unclassified Information," which will provide the specific guidance to contracting officers and associated clauses to implement the DTM in contracts.

We agree that the draft report is appropriately classified.

My point of contact for this response is DoD OIG - (b)(6) at DoD OIG - (b)(6)

Gary D. Guissanie
Acting Deputy Assistant Secretary of Defense
(Identity and Information Assurance)

Consolidated Army Comments

DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT SECRETARY OF THE ARMY
ACQUISITION LOGISTICS AND TECHNOLOGY
103 ARMY PENTAGON
WASHINGTON, DC 20310-0103

SAAL-ZL JUN 16 2010

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR INTELLIGENCE

SUBJECT: Response to Draft DoD Inspector General Report, Project No. D2008-DINT01-0242.001

The enclosed document contains the U.S. Army's reply and comments to the draft report, Results in Brief: DoD Efforts to Protect Critical Program Information: The Army's Warfighter Information Network - Tactical. The Office of the Assistant Secretary of the Army for Acquisition, Logistics and Technology concurs with the findings and offer the enclosed comments to clarify points made in the draft report.

My point of contact is DoD OIG - (b)(6) email: DoD OIG - (b)(6) @us.army.mil.

Encl
Army Recommendations

Wimpy D. Pybus
Deputy Assistant Secretary of the Army
(Acquisition, Logistics and Technology)

Consolidated Army Comments

[redacted]

DoD Inspector General Project No. D2008-DINT01-0242.001

Objective Title: Results in Brief: DoD Efforts to Protect Critical Program Information: The Army's Warfighter Information Network - Tactical

Finding A. Army policy and structure need improved integration, synchronization, and optimization for maximum protection of critical program information (CPI).

Recommendation A: We recommend the Assistant Secretary of the Army (Acquisition, Logistics and Technology) (ASA(ALT)), in conjunction with the Commanding General, Army Material Command, and the Army Deputy Chief of Staff, G-2, review, and develop a plan of action that will result in the most efficient and effective means to integrate, synchronize, and optimize research and technology protection efforts for the Army.

ARMY RESPONSE: Concur with comment. This is a consolidated ASA(ALT), HQDA DCS, G-2, Army Research and Technology Protection Center (ARTPC) and AMC G-2 response. The ASA(ALT)/Defense Industrial Base Cyber Security Office (DIBCSO), HQDA DCS, G-2, ARTPC, and the AMC G-2 continue to collaborate on matters that impact protection of Army CPI. Protection of Army CPI is governed by AR 70-1, DA PAM 70-3 and AR 381-11, which outline the specific responsibilities of the ARTPC and AMC G-2. ASA(ALT), with input from HQDA G-2, ARTPC, and AMC G-2 is developing an Army Regulation that will address these responsibilities in-depth to ensure Army programs properly identify CPI and implement countermeasures to effectively prevent compromise of CPI. ASA(ALT) expects to publish the Army Regulation by 15 December 2010.

Finding B. The Army's Warfighter Information Network - Tactical Program's Efforts to Protect Critical Program Information.

Issue Area One: Ability to identify critical program information

Recommendations:

B1-1. We recommend that the Undersecretary of Defense (Acquisition, Technology and Logistics) (USD(AT&L)), in consultation with the Under Secretary of Defense (Intelligence), the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer, and Component RTP Officials [redacted] OASA ALT - (b)(6)

ARMY RESPONSE: Concur.

[redacted]

Consolidated Army Comments

[redacted]

DoD Inspector General Project No. D2008-DINT01-0242.001

B1-2. We recommend that the Under Secretary of Defense (Acquisition, Technology and Logistics) establish guidance for identifying commercial off-the-shelf/government off-the-shelf components as critical information, to include assessment tools and training.

ARMY RESPONSE: Concur

Issue Area Two: Effectiveness in developing and implementing a Program Protection Plan

Recommendations:

B2-1. We recommend that the Under Secretary of Defense (Acquisition, Technology, and Logistics) provide guidance on model contract language in support of program protection planning to DoD and Component RTP officials.

ARMY RESPONSE: Concur with comment. DoD is seeking comments from Government and industry on potential changes to the Defense Federal Acquisition Regulation Supplement (DFARS) to address requirements for the safeguarding of unclassified information within industry.

B2-2. We recommend that the Director, Defense Security Service provide guidance on model language in the DD Form 254, in order to provide the Defense Security Service with the information they need to protect critical program information.

ARMY RESPONSE: Concur with comment. FAR Clause 52.20-2, Security Requirements binds the contractor to meet the security requirements identified in the National Industrial Security Manual (NISPOM), and further the DD Form 254 shall be used for contracts classified at the Confidential, Secret or Top Secret level. Changes in FAR language and policy will be required to support unclassified contracts containing CPI.

Issue Area Three: Training Efforts for the Protection of Critical Program Information

Recommendation:

B3. We recommend that the Under Secretary of Defense (Acquisition, Technology and Logistics), in collaboration with the Under Secretary of Defense (Intelligence), and the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer develop standardized guidance for training in CPI protection for use by the RTP community.

ARMY RESPONSE: Concur.

Issue Area Four: Use of Resources for the Protection of Critical Program Information

[redacted]

[redacted]

DoD Inspector General Project No. D2008-DINT01-0242.001

No Recommendations

Issue Area Five: Effectiveness of Policies to Protect Critical Program Information

Recommendation:

B5-1. We recommend that the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer, in conjunction with the Under Secretaries of Defense for Acquisition, Technology and Logistics, and for Intelligence, develop and publish security requirements for contractors processing CPI on contractor-owned and controlled information systems.

ARMY RESPONSE: Concur. DoD is seeking comments from Government and industry on potential changes to the Defense Federal Acquisition Regulation Supplement (DFARS) to address requirements for the safeguarding of unclassified information within industry.

Issue Area Six: Ability of Counterintelligence, Intelligence, and Security to Support the Protection of Critical Program Information.

Recommendation:

B6. We recommend that the Director, Defense Security Service, determine and prepare written guidance to:

a. What can and should be contained within the DD 254 for the protection of controlled unclassified CPI; and

b. How program protection should be implemented at the level of subcontractors, and how to verify contractor compliance with the DD Form 254 and the program protection plan.

ARMY RESPONSE: Concur.

Issue Area Seven: Effectiveness of the Foreign Visit Program

No Recommendation.

Issue Area Eight: Application of Horizontal Protection of Critical Program Information

Recommendation:

B8. We recommend that the Under Secretary of Defense (Intelligence), in coordination with the Under Secretary of Defense (Acquisition, Technology and Logistics), and the

[redacted]

Consolidated Army Comments

[redacted]

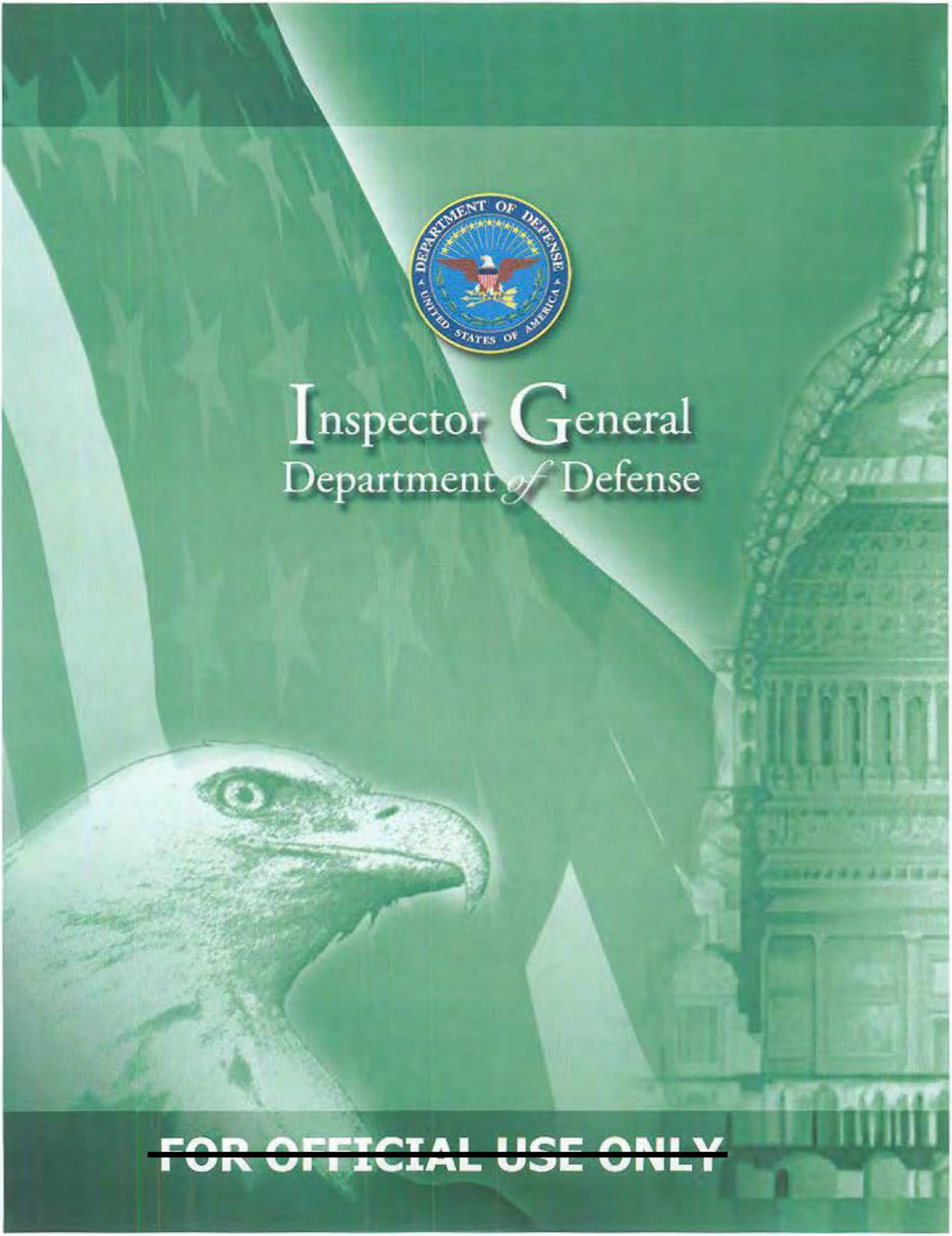
DoD Inspector General Project No. D2008-DINT01-0242.001

Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer, determine the appropriateness of using [redacted] OASA ALT (b)(5)

OASA ALT (b)(5)

ARMY RESPONSE. Concur with comment. OASA ALT - (b)(5) [redacted]

[redacted]


Inspector General
Department of Defense
~~FOR OFFICIAL USE ONLY~~